610:Developments in Privacy & Online Security

Jay T. Angelo
Associate General Counsel
American Management Systems Inc.

Robert L. Rothman
Chief Privacy Officer
General Motors Corporation

Scott R. Shipman
Privacy Counsel
eBay Inc.

Faculty Biographies

Jay T. Angelo

Jay T. Angelo is associate general counsel for American Management Systems in Fairfax, Virginia. His responsibilities include negotiating commercial and government contracts in connection with IT and consulting sales transactions. In addition, Mr. Angelo manages the company's 30-employee contracts staff. In these roles, Mr. Angelo establishes the company's contracting standards and policies, manages outside commercial and government contracts counsel, assists in mergers and acquisitions efforts, and leads internal contracts training efforts.

Prior to joining AMS, Mr. Angelo served for two years as vice president of legal affairs for LGC Wireless, Inc., a wireless infrastructure company in San Jose, California. While at LGC Wireless, Mr. Angelo handled all equipment, software, and services transactions, managed all outside counsel, and assisted the board and CEO in the successful effort to raise and close $30 million in private equity financing. Mr. Angelo previously served as associate general counsel at j2 Global Communications and before that was in private practice at Willkie Farr & Gallagher in Washington, DC.

Mr. Angelo received a BA from Georgetown University and is a graduate of the George Washington University Law School.

Robert L. Rothman

Robert L. Rothman is the chief privacy officer of General Motors Corporation and head of GM's Global Privacy Center.

Mr. Rothman has held a number of positions in GM, most recently as director of eGM's legal affairs in Detroit. Prior to that, he was general counsel of Delphi Automotive Systems in Troy, Michigan, vice president and general counsel of General Motors International Operations in Zurich, general counsel of General Motors Europe, Zurich, Switzerland, head of the legal staff's German office in Rüsselsheim, and attorney-in-charge of overseas legal matters in the Asia/Pacific area.

Mr. Rothman has an AB from the University of Michigan, JD from Ohio State University, and an MBA from Duke University.

Scott R. Shipman

Scott R. Shipman is privacy counsel and head privacy guru for eBay Inc. in San Jose, California. His responsibilities include leading and managing eBay's global privacy practices for customer and employee personal information. Mr. Shipman has first hand experience with cross-border data transfers including the EU, personal information transfers through corporate mergers & acquisitions, GLBA compliance, and many other ecommerce related privacy issues.

Prior to his current position, Mr. Shipman served eBay's legal department by drafting and negotiating corporate contracts, incorporating international subsidiaries, providing sweepstakes and contest compliance reviews, as well as website compliance reviews.

He currently serves on the Santa Clara University School of Law high tech advisory board, is on the IBM privacy manager advisory council, and coordinates a legal high technology internship program at eBay in conjunction with Santa Clara University, School of Law.

Mr. Shipman received a BA from University of Colorado, Boulder, and is a graduate of Santa Clara niversity School of Law.

ams

Global Business and IT Consultants

American Management Systems, Inc.

ACCA Conference 2003

Jay Angelo
Associate General Counsel

Agenda

- AMS, Inc.
- Privacy Regime
- Contracting Advice/Pitfalls

About AMS, Inc.

- Provides Global Business Consulting, IT Solutions and Outsourcing Services
- Nasdaq: AMSY
- Public Sector Practice
  - Federal, State/Local
- Commercial Practice
  - Financial, Telecom, and Health

Financial and Health Practice

- Finance and Health
  - AMS provides proprietary, customized software applications to banks, hospitals, and other similar entities
  - AMS develops, maintains, and operates (on an outsourced basis) these software applications
  - in connection with this work, AMS may have access to personal/private financial or health information of the individual customer of the AMS customer (e.g., the bank or hospital)

Graham Leach Bliley

- GLB requires notice to, and opt-out by, the customer prior to the financial institution's disclosure of "Nonpublic personal information" (NPI) to 3rd party
- Exceptions
  - 3rd party services provided to financial institution
  - 3rd party services provided to customer of financial institution

Graham Leach Bliley – 3rd Party Services
Provided to Financial Institution

- Ex. -- AMS develops and hosts, at its offices in Fairfax, VA, a loan processing application for "XYZ Bank". XYZ Bank transmits to AMS NPI for use in connection with AMS' outsource processing.
  - GLB Privacy Rule: requires a written agreement between XYZ and AMS concerning reuse/redisclosure of NPI that restricts AMS' use of NPI only to extent necessary to perform services
  - GLB Safeguards Rule: requires a written agreement between XYZ and AMS by which AMS commits to maintain NPI under an "adequate" information security program

Graham Leach Bliley – 3rd Party Services

Provided to Financial Institution

- ex. – Joe Customer provides XYZ Bank with his NPI on a mortgage application. On the application he expressly consents to the Bank sharing his NPI with "Insco" so Insco can provide Joe with a quote on homeowners insurance
  - GLB Privacy Rule: does not require any written agreement regarding reuse/redisclosure of NPI
  - GLB Safeguards Rule: requires a written agreement between XYZ and Insco by which Insco commits to maintain NPI under an "adequate" information security program

Health Insurance Portability Accountability Act

- HIPAA requires a regulated health "Covered Entity" to comply with regulatory standards for use and release of customer protected health information (PHI)
- HIPAA also requires written agreement between the Covered Entity and any 3rd party "Business Associate" that establishes a minimum level of privacy safeguards

HIPAA – 3rd Party Services

Provided to Covered Entity

- ex.– "Healthy Hospital" hires AMS to provide its proprietary health care software to the hospital. In so doing, AMS must view and analyze the hospital's customer PHI in order to complete the software customization.
  - HIPAA Privacy Rule: requires Healthy Hospital and AMS to sign a Business Associate Agreement

Contracting Advice/Pitfalls

Are These Obligations Really Fair?

- Private Information Use Restrictions: YES
- Reasonable Reps and Warranties regarding existence of adequate safeguards: YES
- Narrow Audit requirements: MAYBE
  - should be performed by independent auditor/provided to government official
  - costs should be bourne by Financial Inst./Covered Entity

Contracting Advice/Pitfalls

Are These Obligations Really Fair?

- Narrow Indemnity of Bank/Hospital: MAYBE
  - should be triggered by negligent (or worse) performance
  - should only address claims/damages arising against bank/hospital under statute – not third party privacy claims/damages
  - should be limited "to extent bank/hospital's" action gives rise to claim/damage
- Reps, Warranties and Indemnities for 3rd Party: MAYBE
  - ensures that bank has adhered to its regulatory obligations regarding "notice" and "opt-out" and other privacy imperatives
  - protects 3rd party service provider broadly against any potential claims or liability that may result from bank/hospital lapses under any privacy regime, or for 3rd party service provider liability particularly in the event the bank/hospital prescribes the safeguard scheme that must be employed

Contracting Advice/Pitfalls

Are These Obligations Really Fair?

- Disclaimer of 3rd Party Beneficiaries: YES
  - Why?
    - this is essential to affirmatively refute claims of privity between the Service Provider (e.g., AMS) and any individual
    - Congress expressly considered – and rejected – that owners of PHI be made third-party beneficiaries of Business Associate agreements

Contracting Advice/Pitfalls

Are These Obligations Really Fair?

- Broad Indemnity of Bank/Hospital: NO
  - Why?
    - damages will be greater than those otherwise allowable for standard breach of contract
    - obligation to "defend" may give rise to unlimited liability for potentially numerous customer claims against the bank/hospital, no matter how frivolous
    - balance of risks is not appropriate
    - not required or contemplated by regulatory scheme

U.S. Department of Health and Human Services
Office for Civil Rights

Standards for Privacy of Individually Identifiable Health Information

(Unofficial Version)
(45 CFR Parts 160 and 164)

Regulation Text

(December 28, 2000)
as amended:
Part 160
(May 31, 2002)
Parts 160, 164
(August 14, 2002)

Standards for Privacy of Individually Identifiable Health Information Regulation Text, as amended

Table of Contents

Section **Page**

SUBPART B – PREEMPTION OF STATE LAW

SUBPART C – COMPLIANCE AND ENFORCEMENT

PART 164 – SECURITY AND PRIVACY

SUBPART A – GENERAL PROVISIONS

SUBPARTS B-D – [RESERVED]

SUBPART E – PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

PART 160 – GENERAL ADMINISTRATIVE REQUIREMENTS

Authority: Sec. 1171 through 1179 of the Social Security Act, (42 U.S.C. 1320d-1329d-8) as added by sec. 262 of Pub. L. No. 104-191, 110 Stat. 2021-2031 and sec. 264 of Pub. L. No. 104-191 (42 U.S.C. 1320d-2(note)).

Subpart A - General Provisions

§ 160.101 Statutory basis and purpose.
The requirements of this subchapter implement sections 1171 through 1179 of the Social Security Act (the Act), as added by section 262 of Public Law 104-191, and section 264 of Public Law 104-191.

§ 160.102 Applicability.
(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:
(1) A health plan.
(2) A health care clearinghouse.
(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
(b) To the extent required under the Social Security Act, 42 U.S.C. 1320a-7c(a)(5), nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).

§ 160.103 Definitions.
Except as otherwise provided, the following definitions apply to this subchapter:
Act means the Social Security Act.
ANSI stands for the American National Standards Institute.
Business associate:
(1) Except as provided in paragraph (2) of this definition, *business associate* means, with respect to a covered entity, a person who:
(i) On behalf of such covered entity or of an organized health care arrangement (as defined in § 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:
(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
(B) Any other function or activity regulated by this subchapter; or
(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.
(3) A covered entity may be a business associate of another covered entity.
Compliance date means the date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.
Covered entity means:
(1) A health plan.
(2) A health care clearinghouse.
(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
EIN stands for the employer identification number assigned by the Internal Revenue Service, U.S. Department of the Treasury. The EIN is the taxpayer identifying number of an individual or other entity (whether or not an employer) assigned under one or the following:
(1) 26 U.S.C. 6011(b), which is the portion of the Internal Revenue Code dealing with identifying the taxpayer in tax returns and statements, or corresponding provisions of prior law.
(2) 26 U.S.C. 6109, which is the portion of the Internal Revenue Code dealing with identifying numbers in tax returns, statements, and other required documents.
Employer is defined as it is in 26 U.S.C. 3401(d).
Group health plan (also see definition of *health plan* in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:
(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or
(2) Is administered by an entity other than the employer that established and maintains the plan.
HCFA stands for Health Care Financing Administration within the Department of Health and Human Services.
HHS stands for the Department of Health and Human Services.
Health care means care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to, the following:
(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care,

and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information means any information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health insurance issuer (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of *health plan* in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

Health maintenance organization (HMO) (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3) and used in the definition of *health plan* in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(1) *Health plan* includes the following, singly or in combination:

(i) A group health plan, as defined in this section.

(ii) A health insurance issuer, as defined in this section.

(iii) An HMO, as defined in this section.

(iv) Part A or Part B of the Medicare program under title XVIII of the Act.

(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.

(vi) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

(vii) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.

(viii) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(ix) The health care program for active military personnel under title 10 of the United States Code.

(x) The veterans health care program under 38 U.S.C. chapter 17.

(xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)(as defined in 10 U.S.C. 1072(4)).

(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.

(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.

(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.

(xv) The Medicare + Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.

(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.

(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(2) *Health plan* excludes:

(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and

(ii) A government-funded program (other than one listed in paragraph (1)(i)-(xvi)of this definition):

(A) Whose principal purpose is other than providing, or paying the cost of, health care; or

(B) Whose principal activity is:

(*1*) The direct provision of health care to persons; or

(*2*) The making of grants to fund the direct provision of health care to persons.

Implementation specification means specific requirements or instructions for implementing a standard.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Modify or *modification* refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.

Secretary means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Small health plan means a health plan with annual receipts of $5 million or less.

Standard means a rule, condition, or requirement:

(1) Describing the following information for products, systems, services or practices:

(i) Classification of components.

(ii) Specification of materials, performance, or operations; or

(iii) Delineation of procedures; or

(2) With respect to the privacy of

individually identifiable health information.

Standard setting organization (SSO) means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.

State refers to one of the following:

(1) For a health plan established or regulated by Federal law, *State* has the meaning set forth in the applicable section of the United States Code for such health plan.

(2) For all other purposes, *State* means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

Trading partner agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.

(2) Health care payment and remittance advice.

(3) Coordination of benefits.

(4) Health care claim status.

(5) Enrollment and disenrollment in a health plan.

(6) Eligibility for a health plan.

(7) Health plan premium payments.

(8) Referral certification and authorization.

(9) First report of injury.

(10) Health claims attachments.

(11) Other transactions that the Secretary may prescribe by regulation.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

§ 160.104 Modifications.

(a) Except as provided in paragraph (b) of this section, the Secretary may adopt a modification to a standard or implementation specification adopted under this subchapter no more frequently than once every 12 months.

(b) The Secretary may adopt a modification at any time during the first year after the standard or implementation specification is initially adopted, if the Secretary determines that the modification is necessary to permit compliance with the standard or implementation specification.

(c) The Secretary will establish the compliance date for any standard or implementation specification modified under this section.

(1) The compliance date for a modification is no earlier than 180 days after the effective date of the final rule in which the Secretary adopts the modification.

(2) The Secretary may consider the extent of the modification and the time needed to comply with the modification in determining the compliance date for the modification.

(3) The Secretary may extend the compliance date for small health plans, as the Secretary determines is appropriate.

Subpart B - Preemption of State Law

§ 160.201 Applicability.

The provisions of this subpart implement section 1178 of the Act, as added by section 262 of Public Law 104-191.

§ 160.202 Definitions.

For purposes of this subpart, the following terms have the following meanings:

Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

(1) A covered entity would find it impossible to comply with both the State and federal requirements; or

(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub. L. 104-191, as applicable.

More stringent means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:

(i) Required by the Secretary in connection with determining whether a covered entity is in compliance with this subchapter; or

(ii) To the individual who is the subject of the individually identifiable health information.

(2) With respect to the rights of an individual, who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable.

(3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

(4) With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.

(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

Relates to the privacy of individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

State law means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

§ 160.203 General rule and exceptions.

A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law. This general rule applies, except if one or more of the following conditions is met:

(a) A determination is made by the Secretary under § 160.204 that the provision of State law:

(1) Is necessary:

(i) To prevent fraud and abuse related to the provision of or payment for health care;

(ii) To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;

(iii) For State reporting on health care delivery or costs; or

(iv) For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or

(2) Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

(b) The provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.

(c) The provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

(d) The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

§ 160.204 Process for requesting exception determinations.

(a) A request to except a provision of State law from preemption under § 160.203(a) may be submitted to the Secretary. A request by a State must be submitted through its chief elected official, or his or her designee. The request must be in writing and include the following information:

(1) The State law for which the exception is requested;

(2) The particular standard, requirement, or implementation specification for which the exception is requested;

(3) The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;

(4) How health care providers, health plans, and other entities would be affected by the exception;

(5) The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at § 160.203(a); and

(6) Any other information the Secretary may request in order to make the determination.

(b) Requests for exception under this section must be submitted to the Secretary at an address that will be published in the Federal Register. Until the Secretary's determination is made, the standard, requirement, or implementation specification under this subchapter remains in effect.

(c) The Secretary's determination under this section will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met.

§ 160.205 Duration of effectiveness of exception determinations.

An exception granted under this subpart remains in effect until:

(a) Either the State law or the federal standard, requirement, or implementation specification that provided the basis for the exception is materially changed such that the ground for the exception no longer exists; or

(b) The Secretary revokes the exception, based on a determination that the ground supporting the need for the exception no longer exists.

Subpart C - Compliance and Enforcement

§ 160.300 Applicability.

This subpart applies to actions by the Secretary, covered entities, and others with respect to ascertaining the compliance by covered entities with and the enforcement of the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.302 Definitions.

As used in this subpart, terms defined in § 164.501 of this subchapter have the same meanings given to them in that section.

§ 160.304 Principles for achieving compliance.

(a) *Cooperation.* The Secretary will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(b) *Assistance.* The Secretary may provide technical assistance to covered entities to help them comply voluntarily with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.306 Complaints to the Secretary.

(a) *Right to file a complaint.* A person who believes a covered entity is not complying with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter may file a complaint with the Secretary.

(b) *Requirements for filing complaints.* Complaints under this section must meet the following requirements:

(1) A complaint must be filed in writing, either on paper or electronically.

(2) A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(3) A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown.

(4) The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.

(c) *Investigation.* The Secretary may investigate complaints filed under this section. Such investigation may include a review of the pertinent policies, procedures, or practices of the covered entity and of the circumstances regarding any alleged acts or omissions concerning compliance.

§ 160.308 Compliance reviews.

The Secretary may conduct compliance reviews to determine whether covered entities are complying with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.310 Responsibilities of covered entities.

(a) *Provide records and compliance reports.* A covered entity must keep such records and submit such compliance reports, in such time and manner and containing such

information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(b) *Cooperate with complaint investigations and compliance reviews.* A covered entity must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of a covered entity to determine whether it is complying with the applicable requirements of this part 160 and the standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(c) *Permit access to information.*

(1) A covered entity must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity must permit access by the Secretary at any time and without notice.

(2) If any information required of a covered entity under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity must so certify and set forth what efforts it has made to obtain the information.

(3) Protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter, or if otherwise required by law.

§ 160.312 Secretarial action regarding complaints and compliance reviews.

(a) *Resolution where noncompliance is indicated.*

(1) If an investigation pursuant to § 160.306 or a compliance review pursuant to § 160.308 indicates a failure to comply, the Secretary will so inform the covered entity and, if the matter arose from a complaint, the complainant, in writing and attempt to resolve the matter by informal means whenever possible.

(2) If the Secretary finds the covered entity is not in compliance and determines that the matter cannot be resolved by informal means, the Secretary may issue to the covered entity and, if the matter arose from a complaint, to the complainant written findings documenting the non-compliance.

(b) *Resolution when no violation is found.* If, after an investigation or compliance review, the Secretary determines that further action is not warranted, the Secretary will so inform the covered entity and, if the matter arose from a complaint, the complainant in writing.

PART 164 – SECURITY AND PRIVACY

Subpart A – General Provisions

Subparts B-D – [Reserved]

Subpart E – Privacy of Individually Identifiable Health Information

Authority: 42 U.S.C. 1320d-2 and 1320d-4, sec. 264 of Pub. L. No. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2(note)).

Subpart A--General Provisions

§ 164.102 Statutory basis.

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Act and section 264 of Public Law 104-191.

§ 164.104 Applicability.

Except as otherwise provided, the provisions of this part apply to covered entities: health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with any transaction referred to in section 1173(a)(1) of the Act.

§ 164.106 Relationship to other parts.

In complying with the requirements of this part, covered entities are required to comply with the applicable provisions of parts 160 and 162 of this subchapter.

Subpart B-D--[Reserved]

Subpart E - Privacy of Individually Identifiable Health Information

§ 164.500 Applicability.

(a) Except as otherwise provided herein, the standards, requirements, and implementation specifications of this subpart apply to covered entities with respect to protected health information.

(b) Health care clearinghouses must comply with the standards, requirements, and implementation specifications as follows:

(1) When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, the clearinghouse must comply with:

(i) Section 164.500 relating to applicability;

(ii) Section 164.501 relating to definitions;

(iii) Section 164.502 relating to uses and disclosures of protected health information, except that a clearinghouse is prohibited from

using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(iv) Section 164.504 relating to the organizational requirements for covered entities, including the designation of health care components of a covered entity;

(v) Section 164.512 relating to uses and disclosures for which individual authorization or an opportunity to agree or object is not required, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(vi) Section 164.532 relating to transition requirements; and

(vii) Section 164.534 relating to compliance dates for initial implementation of the privacy standards.

(2) When a health care clearinghouse creates or receives protected health information other than as a business associate of a covered entity, the clearinghouse must comply with all of the standards, requirements, and implementation specifications of this subpart.

(c) The standards, requirements, and implementation specifications of this subpart do not apply to the Department of Defense or to any other federal agency, or non-governmental organization acting on its behalf, when providing health care to overseas foreign national beneficiaries.

§ 164.501 Definitions.

As used in this subpart, the following terms have the following meanings:

Correctional institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons held in lawful custody* includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Data aggregation means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

Designated record set means:

(1) A group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) For purposes of this paragraph, the term *record* means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

Direct treatment relationship means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

(v) Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or

entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Indirect treatment relationship means a relationship between an individual and a health care provider in which:

(1) The health care provider delivers health care to the individual based on the orders of another health care provider; and

(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

Individual means the person who is the subject of protected health information.

Inmate means a person incarcerated in or otherwise confined to a correctional institution.

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

(1) Investigate or conduct an official inquiry into a potential violation of law; or

(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Marketing means:

(1) To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:

(i) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.

(ii) For treatment of the individual; or

(iii) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

(2) An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

Organized health care arrangement means:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement; and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

Payment means:

(1) The activities undertaken by:

(i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social security number;

(D) Payment history;

(E) Account number; and

(F) Name and address of the health care provider and/or health plan.

Plan sponsor is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in any medium described in the definition of *electronic media* at § 162.103 of this subchapter; or

(iii) Transmitted or maintained in any other form or medium.

(2) *Protected health information* excludes individually identifiable health information in:

(i) Education records covered by the Family Educational Rights and Privacy Act,

as amended, 20 U.S.C. 1232g;

(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and

(iii) Employment records held by a covered entity in its role as employer.

Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. *Psychotherapy notes* excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Required by law means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

§ 164.502 Uses and disclosures of protected health information: general rules.

(a) *Standard.* A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) *Permitted uses and disclosures.* A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of § 164.502(b), § 164.514(d), and § 164.530(c) with respect to such otherwise permitted or required use or disclosure;

(iv) Pursuant to and in compliance with an authorization that complies with § 164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and

(vi) As permitted by and in compliance with this section, § 164.512, or § 164.514(e), (f), or (g).

(2) *Required disclosures.* A covered entity is required to disclose protected health information:

(i) To an individual, when requested under, and as required by §§ 164.524 or 164.528; and

(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subpart.

(b) *Standard: minimum necessary.*

(1) *Minimum necessary applies.* When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(2) *Minimum necessary does not apply.* This requirement does not apply to:

(i) Disclosures to or requests by a health care provider for treatment;

(ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;

(iii) Uses or disclosures made pursuant to an authorization under § 164.508;

(iv) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;

(v) Uses or disclosures that are required by law, as described by § 164.512(a); and

(vi) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

(c) *Standard: uses and disclosures of protected health information subject to an agreed upon restriction.* A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).

(d) *Standard: uses and disclosures of de-identified protected health information.*

(1) *Uses and disclosures to create de-identified information.* A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

(2) *Uses and disclosures of de-identified information.* Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that:

(i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

(ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

(e)(1) *Standard: disclosures to business associates.*

(i) A covered entity may disclose protected health information to a business associate and may allow a business associate

to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.

(ii) This standard does not apply:

(A) With respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual;

(B) With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of § 164.504(f) apply and are met; or

(C) With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

(iii) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.504(e).

(2) *Implementation specification: documentation.* A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

(f) *Standard: deceased individuals.* A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual.

(g)(1) *Standard: personal representatives.* As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.

(2) *Implementation specification: adults and emancipated minors.* If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(3) *Implementation specification: unemancipated minors.*

(i) If under applicable law a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:

(A) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

(B) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service; or

(C) A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

(ii) Notwithstanding the provisions of paragraph (g)(3)(i) of this section:

(A) If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*;

(B) If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*; and

(C) Where the parent, guardian, or other person acting *in loco parentis*, is not the personal representative under paragraph (g)(3)(i)(A), (B), or (C) of this section and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under § 164.524 to a parent, guardian, or other person acting *in loco parentis*, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

(4) *Implementation specification: deceased individuals.* If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(5) *Implementation specification: abuse, neglect, endangerment situations.* Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:

(i) The covered entity has a reasonable belief that:

(A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

(B) Treating such person as the personal representative could endanger the individual; and

(ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

(h) *Standard: confidential communications.* A covered health care provider or health plan must comply with the applicable requirements of § 164.522(b) in communicating protected health information.

(i) *Standard: uses and disclosures consistent with notice.* A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by § 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in § 164.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

(j) *Standard: disclosures by whistleblowers and workforce member crime victims.*

(1) *Disclosures by whistleblowers.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

(ii) The disclosure is to:

(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.

(2) *Disclosures by workforce members who are victims of a crime.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and

(ii) The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).

§ 164.504 Uses and disclosures: organizational requirements.

(a) *Definitions.* As used in this section:

Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with paragraph (c)(3)(iii) of this section.

Hybrid entity means a single legal entity:

(1) That is a covered entity;

(2) Whose business activities include both covered and non-covered functions; and

(3) That designates health care components in accordance with paragraph (c)(3)(iii) of this section.

Plan administration functions means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

Summary health information means information, that may be individually identifiable health information, and:

(1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and

(2) From which the information described at § 164.514(b)(2)(i) has been deleted, except that the geographic information described in § 164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.

(b) *Standard: health care component.* If a covered entity is a hybrid entity, the requirements of this subpart, other than the requirements of this section, apply only to the health care component(s) of the entity, as specified in this section.

(c)(1) *Implementation specification: application of other provisions.* In applying a provision of this subpart, other than this section, to a hybrid entity:

(i) A reference in such provision to a "covered entity" refers to a health care component of the covered entity;

(ii) A reference in such provision to a "health plan," "covered health care provider," or "health care clearinghouse" refers to a health care component of the covered entity if such health care component performs the functions of a health plan, health care provider, or health care clearinghouse, as applicable; and

(iii) A reference in such provision to "protected health information" refers to protected health information that is created or received by or on behalf of the health care component of the covered entity.

(2) *Implementation specifications: safeguard requirements.* The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this subpart. In particular, and without limiting this requirement, such covered entity must ensure that:

(i) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which this subpart would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

(ii) A component that is described by paragraph (c)(3)(iii)(B) of this section does not use or disclose protected health information that it creates or receives from or on behalf of the health care component in a way prohibited by this subpart; and

(iii) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by this subpart.

(3) *Implementation specifications: responsibilities of the covered entity.* A covered entity that is a hybrid entity has the following responsibilities:

(i) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility to comply with this subpart.

(ii) The covered entity has the responsibility for complying with § 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with this subpart, including the safeguard requirements in paragraph (c)(2) of this section.

(iii) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation as required by § 164.530(j), provided that, if the covered entity designates a health care component or components, it must include any component that would meet the definition of covered entity if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs:

(A) Covered functions; or

(B) Activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.

(d)(1) *Standard: affiliated covered entities.* Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this

subpart.

(2) *Implementation specifications: requirements for designation of an affiliated covered entity.*

(i) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this subpart, if all of the covered entities designated are under common ownership or control.

(ii) The designation of an affiliated covered entity must be documented and the documentation maintained as required by § 164.530(j).

(3) *Implementation specifications: safeguard requirements.* An affiliated covered entity must ensure that:

(i) The affiliated covered entity's use and disclosure of protected health information comply with the applicable requirements of this subpart; and

(ii) If the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, the affiliated covered entity complies with paragraph (g) of this section.

(e)(1) *Standard: business associate contracts.*

(i) The contract or other arrangement between the covered entity and the business associate required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2) or (e)(3) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (e) of this section, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

(A) Terminated the contract or arrangement, if feasible; or

(B) If termination is not feasible, reported the problem to the Secretary.

(2) *Implementation specifications: business associate contracts.* A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;

(D) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(I) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(3) *Implementation specifications: other arrangements.*

(i) If a covered entity and its business associate are both governmental entities:

(A) The covered entity may comply with paragraph (e) of this section by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section.

(B) The covered entity may comply with paragraph (e) of this section, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section.

(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of *business associate* in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph (e), provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(3)(i) of this section, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(4) *Implementation specifications: other requirements for contracts and other arrangements.*

(i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

(A) For the proper management and administration of the business associate; or

(B) To carry out the legal responsibilities of the business associate.

(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:

(A) The disclosure is required by law; or

(B)(*1*) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and

(*2*) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(f)(1) *Standard: Requirements for group health plans.*

(i) Except as provided under paragraph (f)(1)(ii) or (iii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart.

(ii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of :

(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or

(B) Modifying, amending, or terminating the group health plan.

(iii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) *Implementation specifications: requirements for plan documents.* The plan documents of the group health plan must be amended to incorporate provisions to:

(i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.

(ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:

(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

(B) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

(C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;

(D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;

(I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

(J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.

(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:

(A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;

(B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and

(C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.

(3) *Implementation specifications: uses and disclosures.* A group health plan may:

(i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;

(ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;

(iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and

(iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

(g) *Standard: requirements for a covered entity with multiple covered functions.*

(1) A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements, and implementation specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.

(2) A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.

§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

(a) *Standard: Permitted uses and*

disclosures. Except with respect to uses or disclosures that require an authorization under § 164.508(a)(2) and (3), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.

(b) *Standard: Consent for uses and disclosures permitted.*

(1) A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.

(2) Consent, under paragraph (b) of this section, shall not be effective to permit a use or disclosure of protected health information when an authorization, under § 164.508, is required or when another condition must be met for such use or disclosure to be permissible under this subpart.

(c) *Implementation specifications: Treatment, payment, or health care operations.*

(1) A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.

(2) A covered entity may disclose protected health information for treatment activities of a health care provider.

(3) A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.

(4) A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:

(i) For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or

(ii) For the purpose of health care fraud and abuse detection or compliance.

(5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to another covered entity that participates in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

§ 164.508 Uses and disclosures for which an authorization is required.

(a) *Standard: authorizations for uses and disclosures.*

(1) *Authorization required: general rule.* Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

(2) *Authorization required: psychotherapy notes.* Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(i) To carry out the following treatment, payment, or health care operations:

(A) Use by the originator of the psychotherapy notes for treatment;

(B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

(C) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and

(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).

(3) *Authorization required: Marketing.*

(i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:

(A) A face-to-face communication made by a covered entity to an individual; or

(B) A promotional gift of nominal value provided by the covered entity.

(ii) If the marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved.

(b) *Implementation specifications: general requirements.*

(1) *Valid authorizations.*

(i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (c)(1), and (c)(2) of this section, as applicable.

(ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.

(2) *Defective authorizations.* An authorization is not valid, if the document submitted has any of the following defects:

(i) The expiration date has passed or the expiration event is known by the covered entity to have occurred;

(ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c) of this section, if applicable;

(iii) The authorization is known by the covered entity to have been revoked;

(iv) The authorization violates paragraph (b)(3) or (4) of this section, if applicable;

(v) Any material information in the authorization is known by the covered entity to be false.

(3) *Compound authorizations.* An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

(i) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of protected health information for such research or a consent to participate in such research;

(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes;

(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations.

(4) *Prohibition on conditioning of authorizations.* A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

(i) A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health

information for such research under this section;

(ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:

(A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and

(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and

(iii) A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.

(5) *Revocation of authorizations.* An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

(i) The covered entity has taken action in reliance thereon; or

(ii) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

(6) *Documentation.* A covered entity must document and retain any signed authorization under this section as required by § 164.530(j).

(c) *Implementation specifications: Core elements and requirements.*

(1) *Core elements.* A valid authorization under this section must contain at least the following elements:

(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.

(iv) A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

(v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.

(vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

(2) *Required statements.* In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

(i) The individual's right to revoke the authorization in writing, and either:

(A) The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

(B) To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by § 164.520, a reference to the covered entity's notice.

(ii) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:

(A) The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies; or

(B) The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.

(iii) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.

(3) *Plain language requirement.* The authorization must be written in plain language.

(4) *Copy to the individual.* If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.

A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.

(a) *Standard: use and disclosure for facility directories.*

(1) *Permitted uses and disclosure.* Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section, a covered health care provider may:

(i) Use the following protected health information to maintain a directory of individuals in its facility:

(A) The individual's name;

(B) The individual's location in the covered health care provider's facility;

(C) The individual's condition described in general terms that does not communicate specific medical information about the individual; and

(D) The individual's religious affiliation; and

(ii) Disclose for directory purposes such information:

(A) To members of the clergy; or

(B) Except for religious affiliation, to other persons who ask for the individual by name.

(2) *Opportunity to object.* A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.

(3) *Emergency circumstances.*

(i) If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory, if such disclosure is:

(A) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider;

and

(B) In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.

(ii) The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it becomes practicable to do so.

(b) *Standard: uses and disclosures for involvement in the individual's care and notification purposes.*

(1) *Permitted uses and disclosures.*

(i) A covered entity may, in accordance with paragraphs (b)(2) or (3) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.

(ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (3), or (4) of this section, as applicable.

(2) *Uses and disclosures with the individual present.* If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:

(i) Obtains the individual's agreement;

(ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

(iii) Reasonably infers from the circumstances, based the exercise of professional judgment, that the individual does not object to the disclosure.

(3) *Limited uses and disclosures when the individual is not present.* If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

(4) *Use and disclosures for disaster relief purposes.* A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2) and (3) of this section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

A covered entity may use or disclose protected health information without the written authorization of the individual, as described in § 164.508, or the opportunity for the individual to agree or object as described in § 164.510, in the situations covered by this section, subject to the applicable requirements of this section. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, the covered entity's information and the individual's agreement may be given orally.

(a) *Standard: uses and disclosures required by law.*

(1) A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

(2) A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.

(b) *Standard: uses and disclosures for public health activities.*

(1) *Permitted disclosures.* A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to:

(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

(ii) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

(iii) A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

(A) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;

(B) To track FDA-regulated products;

(C) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or

(D) To conduct post marketing surveillance;

(iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

(v) An employer, about an individual who is a member of the workforce of the employer, if:

(A) The covered entity is a covered health care provider who is a member of the workforce of such employer or who provides health care to the individual at the request of the employer:

(*1*) To conduct an evaluation relating to medical surveillance of the workplace; or

(*2*) To evaluate whether the individual

has a work-related illness or injury;

(B) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

(*1*) By giving a copy of the notice to the individual at the time the health care is provided; or

(*2*) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

(2) *Permitted uses.* If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.

(c) *Standard: disclosures about victims of abuse, neglect or domestic violence.*

(1) *Permitted disclosures.* Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

(i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;

(ii) If the individual agrees to the disclosure; or

(iii) To the extent the disclosure is expressly authorized by statute or regulation and:

(A) The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

(B) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

(2) *Informing the individual.* A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if:

(i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

(ii) The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(d) *Standard: uses and disclosures for health oversight activities.*

(1) *Permitted disclosures.* A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

(i) The health care system;

(ii) Government benefit programs for which health information is relevant to beneficiary eligibility;

(iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

(iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.

(2) *Exception to health oversight activities.* For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

(i) The receipt of health care;

(ii) A claim for public benefits related to health; or

(iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

(3) *Joint activities or investigations.* Nothwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.

(4) *Permitted uses.* If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.

(e) *Standard: disclosures for judicial and administrative proceedings.*

(1) *Permitted disclosures.* A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:

(i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or

(ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

(A) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or

(B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.

(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protecting health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The party requesting such information has made a good faith attempt to

provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);

(B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and

(C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:

(*1*) No objections were filed; or

(*2*) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

(iv) For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.

(v) For purposes of paragraph (e)(1) of this section, a *qualified protective order* means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and

(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

(vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section.

(2) *Other uses and disclosures under this section.* The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.

(f) *Standard: disclosures for law enforcement purposes.* A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.

(1) *Permitted disclosures: pursuant to process and as otherwise required by law.* A covered entity may disclose protected health information:

(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or

(ii) In compliance with and as limited by the relevant requirements of:

(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

(B) A grand jury subpoena; or

(C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

(*1*) The information sought is relevant and material to a legitimate law enforcement inquiry;

(*2*) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

(*3*) De-identified information could not reasonably be used.

(2) *Permitted disclosures: limited information for identification and location purposes.* Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

(i) The covered entity may disclose only the following information:

(A) Name and address;

(B) Date and place of birth;

(C) Social security number;

(D) ABO blood type and rh factor;

(E) Type of injury;

(F) Date and time of treatment;

(G) Date and time of death, if applicable; and

(H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

(3) *Permitted disclosure: victims of a crime.* Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to paragraph (b) or (c) of this section, if:

(i) The individual agrees to the disclosure; or

(ii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

(A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;

(B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and

(C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(4) *Permitted disclosure: decedents.* A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.

(5) *Permitted disclosure: crime on premises.* A covered entity may disclose to a law enforcement official protected health

information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

(6) *Permitted disclosure: reporting crime in emergencies.*

(i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

(A) The commission and nature of a crime;

(B) The location of such crime or of the victim(s) of such crime; and

(C) The identity, description, and location of the perpetrator of such crime.

(ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section.

(g) *Standard: uses and disclosures about decedents.*

(1) *Coroners and medical examiners.* A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.

(2) *Funeral directors.* A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.

(h) *Standard: uses and disclosures for cadaveric organ, eye or tissue donation purposes.* A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

(i) *Standard: uses and disclosures for research purposes.*

(1) *Permitted uses and disclosures.* A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:

(i) *Board approval of a waiver of authorization.* The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by §164.508 for use or disclosure of protected health information has been approved by either:

(A) An Institutional Review Board (IRB), established in accordance with 7 CFR 1c.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or

(B) A privacy board that:

(*1*) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;

(*2*) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and

(*3*) Does not have any member participating in a review of any project in which the member has a conflict of interest.

(ii) *Reviews preparatory to research.* The covered entity obtains from the researcher representations that:

(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and

(C) The protected health information for which use or access is sought is necessary for the research purposes.

(iii) *Research on decedent's information.* The covered entity obtains from the researcher:

(A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents;

(B) Documentation, at the request of the covered entity, of the death of such individuals; and

(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

(2) *Documentation of waiver approval.* For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:

(i) *Identification and date of action.* A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;

(ii) *Waiver criteria.* A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

(A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;

(*1*) An adequate plan to protect the identifiers from improper use and disclosure;

(*2*) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

(*3*) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;

(B) The research could not practicably be conducted without the waiver or alteration; and

(C) The research could not practicably be conducted without access to and use of the protected health information.

(iii) *Protected health information needed.* A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board has determined, pursuant to paragraph (i)(2)(ii)(C) of this section;

(iv) *Review and approval procedures.* A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:

(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR

1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110);

(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(*2*) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;

(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and

(v) *Required signature.* The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.

(j) *Standard: uses and disclosures to avert a serious threat to health or safety.*

(1) *Permitted disclosures.* A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:

(i)(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

(B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

(ii) Is necessary for law enforcement authorities to identify or apprehend an individual:

(A) Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or

(B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in § 164.501.

(2) *Use or disclosure not permitted.* A use or disclosure pursuant to paragraph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:

(i) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or counseling or therapy; or

(ii) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in paragraph (j)(2)(i) of this section.

(3) *Limit on information that may be disclosed.* A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.

(4) *Presumption of good faith belief.* A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

(k) *Standard: uses and disclosures for specialized government functions.*

(1) *Military and veterans activities.*

(i) *Armed Forces personnel.* A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the **Federal Register** the following information:

(A) Appropriate military command authorities; and

(B) The purposes for which the protected health information may be used or disclosed.

(ii) *Separation or discharge from military service.* A covered entity that is a component of the Departments of Defense or Transportation may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

(iii) *Veterans.* A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.

(iv) *Foreign military personnel.* A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the **Federal Register** pursuant to paragraph (k)(1)(i) of this section.

(2) *National security and intelligence activities.* A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority (e.g., Executive Order 12333).

(3) *Protective services for the President and others.* A covered entity may disclose protected health information to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or to for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

(4) *Medical suitability determinations.* A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the officials in the Department of State who need access to such information for the following purposes:

(i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12698;

(ii) As necessary to determine worldwide availability or availability for mandatory

service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or

(iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.

(5) *Correctional institutions and other law enforcement custodial situations.*

(i) *Permitted disclosures.* A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

(A) The provision of health care to such individuals;

(B) The health and safety of such individual or other inmates;

(C) The health and safety of the officers or employees of or others at the correctional institution;

(D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;

(E) Law enforcement on the premises of the correctional institution; and

(F) The administration and maintenance of the safety, security, and good order of the correctional institution.

(ii) *Permitted uses.* A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.

(iii) *No application after release.* For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

(6) *Covered entities that are government programs providing public benefits.*

(i) A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.

(ii) A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

(l) *Standard: disclosures for workers' compensation.* A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

§ 164.514 Other requirements relating to uses and disclosures of protected health information.

(a) *Standard: de-identification of protected health information.* Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

(b) *Implementation specifications: requirements for de-identification of protected health information.* A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination; or

(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(*1*) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(*2*) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

(c) *Implementation specifications: re-identification.* A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

(1) *Derivation.* The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

(2) *Security.* The covered entity does not use or disclose the code or other means of

record identification for any other purpose, and does not disclose the mechanism for re-identification.

(d)(1) *Standard: minimum necessary requirements.* In order to comply with § 164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information.

(2) *Implementation specifications: minimum necessary uses of protected health information.*

(i) A covered entity must identify:

(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and

(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.

(3) *Implementation specification: minimum necessary disclosures of protected health information.*

(i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

(ii) For all other disclosures, a covered entity must:

(A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

(A) Making disclosures to public officials that are permitted under § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

(B) The information is requested by another covered entity;

(C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

(D) Documentation or representations that comply with the applicable requirements of § 164.512(i) have been provided by a person requesting the information for research purposes.

(4) *Implementation specifications: minimum necessary requests for protected health information.*

(i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

(ii) For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

(iii) For all other requests, a covered entity must:

(A) Develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(5) *Implementation specification: other content requirement.* For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

(e) (1) *Standard: Limited data set.* A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2) and (e)(3) of this section, if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section.

(2) *Implementation specification: Limited data set:* A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

(i) Names;

(ii) Postal address information, other than town or city, State, and zip code;

(iii) Telephone numbers;

(iv) Fax numbers;

(v) Electronic mail addresses;

(vi) Social security numbers;

(vii) Medical record numbers;

(viii) Health plan beneficiary numbers;

(ix) Account numbers;

(x) Certificate/license numbers;

(xi) Vehicle identifiers and serial numbers, including license plate numbers;

(xii) Device identifiers and serial numbers;

(xiii) Web Universal Resource Locators (URLs);

(xiv) Internet Protocol (IP) address numbers;

(xv) Biometric identifiers, including finger and voice prints; and

(xvi) Full face photographic images and any comparable images.

(3) *Implementation specification: Permitted purposes for uses and disclosures.*

(i) A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations.

(ii) A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.

(4) *Implementation specifications: Data use agreement.*

(i) *Agreement required.* A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes.

(ii) *Contents.* A data use agreement between the covered entity and the limited data set recipient must:

(A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the

information in a manner that would violate the requirements of this subpart, if done by the covered entity;

(B) Establish who is permitted to use or receive the limited data set; and

(C) Provide that the limited data set recipient will:

(*1*) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

(*2*) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

(*3*) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

(*4*) Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

(*5*) Not identify the information or contact the individuals.

(iii) *Compliance.*

(A) A covered entity is not in compliance with the standards in paragraph (e) of this section if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

(*1*) Discontinued disclosure of protected health information to the recipient; and

(*2*) Reported the problem to the Secretary.

(B) A covered entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with the standards, implementation specifications, and requirements of paragraph (e) of this section.

(f)(1) *Standard: uses and disclosures for fundraising.* A covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:

(i) Demographic information relating to an individual; and

(ii) Dates of health care provided to an individual.

(2) *Implementation specifications: fundraising requirements.*

(i) The covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by § 164.520(b)(1)(iii)(B) is included in the covered entity's notice;

(ii) The covered entity must include in any fundraising materials it sends to an individual under this paragraph a description of how the individual may opt out of receiving any further fundraising communications.

(iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.

(g) *Standard: uses and disclosures for underwriting and related purposes.* If a health plan receives protected heath information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such protected health information for any other purpose, except as may be required by law.

(h)(1) *Standard: verification requirements.* Prior to any disclosure permitted by this subpart, a covered entity must:

(i) Except with respect to disclosures under § 164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and

(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.

(2) *Implementation specifications: verification.*

(i) *Conditions on disclosures.* If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

(A) The conditions in § 164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

(B) The documentation required by § 164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with § 164.512(i)(2)(i) and (v).

(ii) *Identity of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

(B) If the request is in writing, the request is on the appropriate government letterhead; or

(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(iii) *Authority of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

(iv) *Exercise of professional judgment.* The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with § 164.510 or acts on a good faith belief in making a disclosure in accordance with § 164.512(j).

§ 164.520 Notice of privacy practices for

protected health information.

(a) *Standard: notice of privacy practices.*

(1) *Right to notice.* Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

(2) *Exception for group health plans.*

(i) An individual enrolled in a group health plan has a right to notice:

(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or

(B) From the health insurance issuer or HMO with respect to the group health plan though which such individuals receive their health benefits under the group health plan.

(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in § 164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:

(A) Maintain a notice under this section; and

(B) Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.

(iii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in § 164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.

(3) *Exception for inmates.* An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.

(b) *Implementation specifications: content of notice.*

(1) *Required elements.* The covered entity must provide a notice that is written in plain language and that contains the elements required by this paragraph.

(i) *Header.* The notice must contain the following statement as a header or otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

(ii) *Uses and disclosures.* The notice must contain:

(A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations.

(B) A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written authorization.

(C) If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law as defined in § 160.202.

(D) For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law.

(E) A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as provided by § 164.508(b)(5).

(iii) *Separate statements for certain uses or disclosures.* If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement, as applicable, that:

(A) The covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other heath-related benefits and services that may be of interest to the individual;

(B) The covered entity may contact the individual to raise funds for the covered entity; or

(C) A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.

(iv) *Individual rights.* The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:

(A) The right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction;

(B) The right to receive confidential communications of protected health information as provided by § 164.522(b), as applicable;

(C) The right to inspect and copy protected health information as provided by § 164.524;

(D) The right to amend protected health information as provided by § 164.526;

(E) The right to receive an accounting of disclosures of protected health information as provided by § 164.528; and

(F) The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request.

(v) *Covered entity's duties.* The notice must contain:

(A) A statement that the covered entity is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information;

(B) A statement that the covered entity is required to abide by the terms of the notice currently in effect; and

(C) For the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.

(vi) *Complaints.* The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.

(vii) *Contact.* The notice must contain the name, or title, and telephone number of a

person or office to contact for further information as required by § 164.530(a)(1)(ii).

(viii) *Effective date.* The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

(2) *Optional elements.*

(i) In addition to the information required by paragraph (b)(1) of this section, if a covered entity elects to limit the uses or disclosures that it is permitted to make under this subpart, the covered entity may describe its more limited uses or disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by § 164.512(j)(1)(i).

(ii) For the covered entity to apply a change in its more limited uses and disclosures to protected health information created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), the notice must include the statements required by paragraph (b)(1)(v)(C) of this section.

(3) *Revisions to the notice.* The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

(c) *Implementation specifications: provision of notice.* A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(3) of this section, as applicable.

(1) *Specific requirements for health plans.*

(i) A health plan must provide notice:

(A) No later than the compliance date for the health plan, to individuals then covered by the plan;

(B) Thereafter, at the time of enrollment, to individuals who are new enrollees; and

(C) Within 60 days of a material revision to the notice, to individuals then covered by the plan.

(ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

(iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.

(iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.

(2) *Specific requirements for certain covered health care providers.* A covered health care provider that has a direct treatment relationship with an individual must:

(i) Provide the notice:

(A) No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or

(B) In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.

(ii) Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained;

(iii) If the covered health care provider maintains a physical service delivery site:

(A) Have the notice available at the service delivery site for individuals to request to take with them; and

(B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and

(iv) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(iii) of this section, if applicable.

(3) *Specific requirements for electronic notice.*

(i) A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

(ii) A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.

(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. The requirements in paragraph (c)(2)(ii) of this section apply to electronic notice.

(iv) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

(d) *Implementation specifications: joint notice by separate covered entities.* Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that:

(1) The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement;

(2) The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity; and

(i) Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;

(ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and

(iii) If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.

(3) The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of paragraph (c) of this section with respect to

all others covered by the joint notice.

(e) *Implementation specifications: Documentation.* A covered entity must document compliance with the notice requirements, as required by § 164.530(j), by retaining copies of the notices issued by the covered entity and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment, in accordance with paragraph (c)(2)(ii) of this section.

§ 164.522 Rights to request privacy protection for protected health information.

(a)(1) *Standard: right of an individual to request restriction of uses and disclosures.*

(i) A covered entity must permit an individual to request that the covered entity restrict:

(A) Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and

(B) Disclosures permitted under § 164.510(b).

(ii) A covered entity is not required to agree to a restriction.

(iii) A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.

(iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.

(v) A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(ii), 164.510(a) or 164.512.

(2) *Implementation specifications: terminating a restriction.* A covered entity may terminate its agreement to a restriction, if:

(i) The individual agrees to or requests the termination in writing;

(ii) The individual orally agrees to the termination and the oral agreement is documented; or

(iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to protected health information created or received after it has so informed the individual.

(3) *Implementation specification: documentation.* A covered entity that agrees to a restriction must document the restriction in accordance with § 164.530(j).

(b)(1) *Standard: confidential communications requirements.*

(i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.

(ii) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

(2) *Implementation specifications: conditions on providing confidential communications.*

(i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.

(ii) A covered entity may condition the provision of a reasonable accommodation on:

(A) When appropriate, information as to how payment, if any, will be handled; and

(B) Specification of an alternative address or other method of contact.

(iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

(iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

§ 164.524 Access of individuals to protected health information.

(a) *Standard: access to protected health information.*

(1) *Right of access.* Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:

(i) Psychotherapy notes;

(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

(iii) Protected health information maintained by a covered entity that is:

(A) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or

(B) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).

(2) *Unreviewable grounds for denial.* A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.

(i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section.

(ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

(iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

(iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

(v) An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of

confidentiality and the access requested would be reasonably likely to reveal the source of the information.

(3) *Reviewable grounds for denial.* A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:

(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

(iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

(4) *Review of a denial of access.* If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.

(b) *Implementation specifications: requests for access and timely action.*

(1) *Individual's request for access.* The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.

(2) *Timely action by the covered entity.*

(i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.

(A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.

(B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.

(ii) If the request for access is for protected health information that is not maintained or accessible to the covered entity on-site, the covered entity must take an action required by paragraph (b)(2)(i) of this section by no later than 60 days from the receipt of such a request.

(iii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) or (ii) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) or (ii) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for access.

(c) *Implementation specifications: provision of access.* If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) *Providing the access requested.* The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.

(2) *Form of access requested.*

(i) The covered entity must provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual.

(ii) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:

(A) The individual agrees in advance to such a summary or explanation; and

(B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

(3) *Time and manner of access.* The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

(4) *Fees.* If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

(i) Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual;

(ii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and

(iii) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(ii) of this section.

(d) *Implementation specifications: denial of access.* If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) *Making other information accessible.* The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.

(2) *Denial.* The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:

(i) The basis for the denial;

(ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description

of how the individual may exercise such review rights; and

(iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in § 164.530(d) or to the Secretary pursuant to the procedures in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(3) *Other responsibility.* If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.

(4) *Review of denial requested.* If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

(e) *Implementation specification: documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The designated record sets that are subject to access by individuals; and

(2) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

§ 164.526 Amendment of protected health information.

(a) *Standard: right to amend.*

(1) *Right to amend.* An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

(2) *Denial of amendment.* A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

(i) Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;

(ii) Is not part of the designated record set;

(iii) Would not be available for inspection under § 164.524; or

(iv) Is accurate and complete.

(b) *Implementation specifications: requests for amendment and timely action.*

(1) *Individual's request for amendment.* The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.

(2) *Timely action by the covered entity.*

(i) The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

(A) If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.

(B) If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.

(ii) If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for an amendment.

(c) *Implementation specifications: accepting the amendment.* If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Making the amendment.* The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) *Informing the individual.* In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

(3) *Informing others.* The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and

(ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

(d) *Implementation specifications: denying the amendment.* If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Denial.* The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:

(i) The basis for the denial, in accordance with paragraph (a)(2) of this section;

(ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

(iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

(iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.530(d) or to the Secretary pursuant to the procedures established in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in §164.530(a)(1)(ii).

(2) *Statement of disagreement.* The covered entity must permit the individual to

submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

(3) *Rebuttal statement.* The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.

(4) *Recordkeeping.* The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) *Future disclosures.*

(i) If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.

(ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.

(iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.

(e) *Implementation specification: actions on notices of amendment.* A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.

(f) *Implementation specification: documentation.* A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by § 164.530(j).

§ 164.528 Accounting of disclosures of protected health information.

(a) *Standard: right to an accounting of disclosures of protected health information.*

(1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

(i) To carry out treatment, payment and health care operations as provided in § 164.506;

(ii) To individuals of protected health information about them as provided in § 164.502;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502;

(iv) Pursuant to an authorization as provided in § 164.508;

(v) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in § 164.510;

(vi) For national security or intelligence purposes as provided in § 164.512(k)(2);

(vii) To correctional institutions or law enforcement officials as provided in § 164.512(k)(5);

(viii) As part of a limited data set in accordance with § 164.514(e); or

(ix) That occurred prior to the compliance date for the covered entity.

(2)(i) The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

(ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:

(A) Document the statement, including the identity of the agency or official making the statement;

(B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

(C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.

(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

(b) *Implementation specifications: content of the accounting.* The covered entity must provide the individual with a written accounting that meets the following requirements.

(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.

(2) Except as otherwise provided by paragraphs (b)(3) or (b)(4) of this section, the accounting must include for each disclosure:

(i) The date of the disclosure;

(ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(iii) A brief description of the protected health information disclosed; and

(iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) or 164.512, if any.

(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under §§ 164.502(a)(2)(ii) or 164.512, the accounting may, with respect to such multiple disclosures, provide:

(i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;

(ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and

(iii) The date of the last such disclosure during the accounting period.

(4)(i) If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose in

accordance with § 164.512(i) for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide:

(A) The name of the protocol or other research activity;

(B) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

(C) A brief description of the type of protected health information that was disclosed;

(D) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

(E) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

(F) A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.

(ii) If the covered entity provides an accounting for research disclosures, in accordance with paragraph (b)(4) of this section, and if it is reasonably likely that the protected health information of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

(c) *Implementation specifications: provision of the accounting.*

(1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.

(i) The covered entity must provide the individual with the accounting requested; or

(ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and

(B) The covered entity may have only one such extension of time for action on a request for an accounting.

(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

(d) *Implementation specification: documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section;

(2) The written accounting that is provided to the individual under this section; and

(3) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

§ 164.530 Administrative requirements.

(a)(1) *Standard: personnel designations.*

(i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.

(2) *Implementation specification: personnel designations.* A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

(b)(1) *Standard: training.* A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.

(2) *Implementation specifications: training.*

(i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;

(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

(c)(1) *Standard: safeguards.* A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2) *Implementation specification: safeguards.*

(i) A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

(d)(1) *Standard: complaints to the covered entity.* A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart or its compliance with such policies and procedures or the requirements of this subpart.

(2) *Implementation specification: documentation of complaints.* As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.

(e)(1) *Standard: sanctions.* A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.

(2) *Implementation specification: documentation.* As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.

(f) *Standard: mitigation.* A covered entity must mitigate, to the extent practicable, any

harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

(g) *Standard: refraining from intimidating or retaliatory acts.* A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

(1) *Individuals.* Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by this subpart, including the filing of a complaint under this section;

(2) *Individuals and others.* Any individual or other person for:

(i) Filing of a complaint with the Secretary under subpart C of part 160 of this subchapter;

(ii) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or

(iii) Opposing any act or practice made unlawful by this subpart, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of this subpart.

(h) *Standard: waiver of rights.* A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter or this subpart as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

(i)(1) *Standard: policies and procedures.* A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.

(2) *Standard: changes to policies or procedures.*

(i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart;

(ii) When a covered entity changes a privacy practice that is stated in the notice described in § 164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with § 164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or

(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.

(3) *Implementation specification: changes in law.* Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by § 164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with § 164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.

(4) *Implementation specifications: changes to privacy practices stated in the notice.*

(i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:

(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;

(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and

(C) Revise the notice as required by § 164.520(b)(3) to state the changed practice and make the revised notice available as required by § 164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.

(ii) If a covered entity has not reserved its right under § 164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:

(A) Such change meets the implementation specifications in paragraphs (i)(4)(i)(A)-(C) of this section; and

(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.

(5) *Implementation specification: changes to other policies or procedures.* A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by § 164.520, provided that:

(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and

(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.

(j)(1) *Standard: documentation.* A covered entity must:

(i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;

(ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and

(iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.

(2) *Implementation specification: retention period.* A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.

(k) *Standard: group health plans.*

(1) A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:

(i) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and

(ii) The group health plan does not create or receive protected health information, except for:

(A) Summary health information as defined in § 164.504(a); or

(B) Information on whether the individual is participating in the group health

plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with § 164.504(f).

§ 164.532 Transition provisions.

(a) *Standard: Effect of prior authorizations.* Notwithstanding §§ 164.508 and 164.512(i), a covered entity may use or disclose protected health information, consistent with paragraphs (b) and (c) of this section, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, or a waiver of informed consent by an IRB.

(b) *Implementation specification: Effect of prior authorization for purposes other than research.* Notwithstanding any provisions in § 164.508, a covered entity may use or disclose protected health information that it created or received prior to the applicable compliance date of this subpart pursuant to an authorization or other express legal permission obtained from an individual prior to the applicable compliance date of this subpart, provided that the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction in accordance with § 164.522(a).

(c) *Implementation specification: Effect of prior permission for research.* Notwithstanding any provisions in §§ 164.508 and 164.512(i), a covered entity may, to the extent allowed by one of the following permissions, use or disclose, for research, protected health information that it created or received either before or after the applicable compliance date of this subpart, provided that there is no agreed-to restriction in accordance with § 164.522(a), and the covered entity has obtained, prior to the applicable compliance date, either:

(1) An authorization or other express legal permission from an individual to use or disclose protected health information for the research;

(2) The informed consent of the individual to participate in the research; or

(3) A waiver, by an IRB, of informed consent for the research, in accordance with 7 CFR 1c.116(d), 10 CFR 745.116(d), 14 CFR 1230.116(d), 15 CFR 27.116(d), 16 CFR 1028.116(d), 21 CFR 50.24, 22 CFR 225.116(d), 24 CFR 60.116(d), 28 CFR 46.116(d), 32 CFR 219.116(d), 34 CFR 97.116(d), 38 CFR 16.116(d), 40 CFR 26.116(d), 45 CFR 46.116(d), 45 CFR 690.116(d), or 49 CFR 11.116(d), provided that a covered entity must obtain authorization in accordance with § 164.508 if, after the compliance date, informed consent is sought from an individual participating in the research.

(d) *Standard: Effect of prior contracts or other arrangements with business associates.* Notwithstanding any other provisions of this subpart, a covered entity, other than a small health plan, may disclose protected health information to a business associate and may allow a business associate to create, receive, or use protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does not comply with §§ 164.502(e) and 164.504(e) consistent with the requirements, and only for such time, set forth in paragraph (e) of this section.

(e) *Implementation specification: Deemed compliance.*

(1) *Qualification.* Notwithstanding other sections of this subpart, a covered entity, other than a small health plan, is deemed to be in compliance with the documentation and contract requirements of §§ 164.502(e) and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if:

(i) Prior to October 15, 2002, such covered entity has entered into and is operating pursuant to a written contract or other written arrangement with a business associate for such business associate to perform functions or activities or provide services that make the entity a business associate; and

(ii) The contract or other arrangement is not renewed or modified from October 15, 2002, until the compliance date set forth in § 164.534.

(2) *Limited deemed compliance period.* A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section, shall be deemed compliant until the earlier of:

(i) The date such contract or other arrangement is renewed or modified on or after the compliance date set forth in § 164.534; or

(ii) April 14, 2004.

(3) *Covered entity responsibilities.* Nothing in this section shall alter the requirements of a covered entity to comply with Part 160, Subpart C of this subchapter and §§ 164.524, 164.526, 164.528, and 164.530(f) with respect to protected health information held by a business associate.

§ 164.534 Compliance dates for initial implementation of the privacy standards.

(a) *Health care providers.* A covered health care provider must comply with the applicable requirements of this subpart no later than April 14, 2003.

(b) *Health plans.* A health plan must comply with the applicable requirements of this subpart no later than the following date, as applicable:

(1) *Health plans other than small health plans* – April 14, 2003.

(2) *Small health plans* – April 14, 2004.

(c) *Health care clearinghouses.* A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 14, 2003.

Federal Register

Thursday,
May 23, 2002

Part VII

Federal Trade Commission

16 CFR Part 314
Standards for Safeguarding Customer Information; Final Rule

36484 Federal Register / Vol. 67, No. 100 / Thursday, May 23, 2002 / Rules and Regulations

FEDERAL TRADE COMMISSION

16 CFR Part 314

RIN 3084 AA87

Standards for Safeguarding Customer Information

AGENCY: Federal Trade Commission.

ACTION: Final rule.

SUMMARY: The Federal Trade Commission ("FTC" or "Commission") is issuing a final Safeguards Rule, as required by section 501(b) of the Gramm-Leach-Bliley Act ("G–L–B Act" or "Act"), to establish standards relating to administrative, technical and physical information safeguards for financial institutions subject to the Commission's jurisdiction. As required by section 501(b), the standards are intended to: Ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

EFFECTIVE DATE: This rule is effective on May 23, 2003.

FOR FURTHER INFORMATION CONTACT: Laura D. Berger, Attorney, Division of Financial Practices, (202) 326–3224.

SUPPLEMENTARY INFORMATION: The contents of this preamble are listed in the following outline:

Section A. Background

On November 12, 1999, President Clinton signed the G–L–B Act (Pub. L. 106–102) into law. The purpose of the Act was to reform and modernize the banking industry by eliminating existing barriers between banking and commerce. The Act permits banks to engage in a broad range of activities, including insurance and securities brokering, with new affiliated entities. Subtitle A of Title V of the Act, captioned "Disclosure of Nonpublic Personal Information," limits the instances in which a financial institution may disclose nonpublic personal information about a consumer to nonaffiliated third parties, and requires a financial institution to disclose certain privacy policies and practices with respect to its information sharing with both affiliates and nonaffiliated third parties. On May 12, 2000, the Commission issued a final rule, Privacy of Consumer Financial Information, 16 CFR part 313, which implemented Subtitle A as it relates to these requirements (hereinafter "Privacy Rule").[1] The Privacy Rule took effect on November 13, 2000, and full compliance was required on or before July 1, 2001.

Subtitle A of Title V also requires the Commission and other federal agencies to establish standards for financial institutions relating to administrative, technical, and physical safeguards for certain information.[2] *See* 15 U.S.C. 6801(b), 6805(b)(2). As described in the Act, the objectives of these standards are to: (1) Ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. *See* 15 U.S.C. 6801(b)(1)–(3). The Act does not require all of the agencies to coordinate in developing their safeguards standards, and does not impose a deadline to establish them.[3] Although the Act permits most of the agencies to develop their safeguards standards by issuing guidelines, it requires the SEC and the Commission to proceed by rule.[4]

On September 7, 2000, the Commission issued for publication in the **Federal Register** a Advanced Notice of Proposed Rulemaking ("the ANPR") on the scope and potential requirements of a Safeguards Rule for the financial institutions subject to its jurisdiction.[5] The Commission received thirty comments in response to the ANPR. Based on these comments, as well as the safeguards standards already issued by the other GLB agencies, the Commission issued a Notice of Proposed Rulemaking respecting Standards for Safeguarding Customer Information ("the proposal" or "the Proposed Rule") on August 7, 2001.[6] In response to the proposal, the Commission received forty-four comments from a variety of interested parties. The Commission now issues a final rule governing the safeguarding of customer records and information for the financial institutions subject to its jurisdiction ("Safeguards Rule").

Like the proposal, the Final Rule requires each financial institution to develop a written information security program that is appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue. As described below, each information security program must include certain basic elements to ensure that it addresses the relevant aspects of a financial institution's operations and that it keeps pace with developments that may have a material impact on its safeguards. In developing the Final Rule, the Commission carefully weighed the comments, including concerns expressed about the ability of smaller and less sophisticated financial institutions to meet the Rule's requirements. It also sought to ensure that the Rule mirrored the requirements of the guidelines already established by the NCUA and the other banking agencies (collectively, "the Banking Agency Guidelines"),[7] with adjustments as needed to clarify the Rule's scope and accommodate the diverse range of entities covered by the Commission's Rule. The Commission believes that the Final Rule strikes an appropriate balance between allowing flexibility to financial institutions and establishing standards for safeguarding customer information that are consistent with the Act's goals. As described below, the Commission will issue educational materials in connection with the Rule in order to assist businesses—and in particular, small entities—to comply with its requirements without imposing undue burdens.

[1] The rule was published in the **Federal Register** at 65 FR 33646 (May 24, 2000).

[2] The other agencies responsible for establishing safeguards standards are: the Office of the Comptroller of the Currency ("OCC"); the Board of Governors of the Federal Reserve System ("Board"); the Federal Deposit Insurance Corporation ("FDIC"); the Office of Thrift Supervision ("OTS"); the National Credit Union Administration ("NCUA"); the Secretary of the Treasury ("Treasury"); and the Securities and Exchange Commission ("SEC").

[3] By contrast, section 504 of the Act required the Agencies to work together to issue consistent and comparable rules to implement the Act's privacy provisions.

[4] The NCUA and the remaining banking agencies—the OCC, the Board, the FDIC, and OTS—have already issued final guidelines that are substantively identical. 66 FR 8152 (Jan. 30, 2001); 66 FR 8616 (Feb. 1, 2001). The SEC also adopted a final safeguards rule as part of its Privacy of Consumer Financial Information Final Rule (hereinafter "SEC rule"). *See www.sec.gov/rules/final/34–42974.htm* (June 29, 2000).

[5] 65 FR 54186.

[6] 66 FR 41162. In addition to considering the Banking Agency Guidelines, the Commission also considered the Final Report that was issued by the Federal Trade Commission Advisory Committee on Online Access and Security on May 15, 2000 ("Advisory Committee's Report" or "ACR"). Although the Advisory Committee's Report addressed security only in the online context, the Commission believes that its principles have general relevance to information safeguards.

[7] *See supra* n.4.

Section B. Overview of Comments Received

The comments received were submitted by a variety of interested parties: [8] twenty-eight were from trade or other associations or companies related to financial or Internet-related services; [9] six were from corporations or associations related to higher education or the funding of student loans; [10] five were from individuals; [11] three were from information security companies; [12] two were from consumer reporting agencies; [13] and one was from a non-profit association of consumer agencies.[14]

The majority of commenters supported the proposal overall, citing its flexibility [15] and similarity to the Banking Agency Guidelines.[16] However, as discussed below, commenters expressed different views on issues concerning the Rule's scope—in particular, whether financial institutions should be responsible for the safeguards of their affiliates and service providers and whether the Rule should apply to a financial institution that has no customer relationship but receives customer information from another financial institution. In addition, a number of commenters asked that compliance with alternative standards be deemed compliance with the Rule and/or sought to exclude certain entities from the Rule's definition of "service provider." Finally, numerous commenters urged that the Commission provide guidance to businesses—particularly smaller businesses—on how to comply with the Rule without incurring undue expense.[17] As discussed in detail below, comments on all of these issues were instrumental in shaping the Final Rule.

Additional comments, and the Commission's responses thereto, are discussed in the following Section-by-Section analysis.

Section C. Section-by-Section Analysis

Consistent with the proposal, the Safeguards Rule will be part 314 of 16 CFR, to be entitled "Standards for Safeguarding Customer Information." This Part will follow the Privacy Rule, which is contained in part 313 of 16 CFR. The following is a section-by-section analysis of the Final Rule.

Section 314.1: Purpose and Scope

Paragraph 314.1(a) states that the Rule is intended to establish standards for financial institutions to develop, implement and maintain administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. This paragraph also states the statutory authority for the proposed Rule. No comments addressed this provision, and the Commission has made no changes to it.

Paragraph 314.1(b) sets forth the scope of the Rule, which applies to the handling of customer information by all financial institutions over which the FTC has jurisdiction. Because, as noted below, "financial institution" is defined as it is in section 509(3)(A) of the Act and the Privacy Rule, the Rule covers a wide range of entities, including: non-depository lenders; consumer reporting agencies; debt collectors; data processors; courier services; retailers that extend credit by issuing credit cards to consumers; personal property or real estate appraisers; check-cashing businesses; mortgage brokers, and any other entity that meets this definition.[18]

Consistent with the proposal, the Safeguards Rule covers any financial institution that is handling "customer information"—*i.e.*, not only financial institutions that collect nonpublic personal information from their own customers, but also financial institutions that receive customer information from other financial institutions.

Comments were split on whether the Rule should apply to customer information that a financial institution receives from another financial institution. A number of commenters agreed that such recipients should be required to maintain safeguards, citing the added protections provided by this requirement.[19] However, one of these commenters expressed concern that a recipient financial institution could be subject to multiple safeguards standards or even required to prepare multiple written safeguards plans if that financial institution also acts as a service provider or is subject to other laws, such as the Fair Credit Reporting Act, that impose confidentiality requirements.[20] In addition, some commenters opposed covering recipients on the grounds that such coverage is: (1) Beyond the intent of section 501(a), which refers to a financial institution's obligation to "its customers;" (2) unnecessary in light of the Rule's separate treatment of service providers and affiliates; and/or (3) too burdensome.[21]

After considering the comments, the Commission has determined that covering recipient financial institutions is consistent with the purpose and language of the Act. The Commission believes that imposing safeguards obligations as to customer information that a financial institution receives about another institution's customers is the most reasonable reading of the statutory language and clearly furthers the express congressional policy to

[8] These comments are available on the Commission's Web site, at www.ftc.gov.

[9] ACA International ("ACA"); America's Community Bankers ("ACB"); Associated Credit Bureaus, now renamed the Consumer Data Industry Association ("CDIA"); BITS/Financial Services Roundtable ("BITS"); Commerce Bankshares, Inc.; Credit Union Nat'l Ass'n ("CUNA"); Council of Ins. Agents and Brokers; Debt Buyers Ass'n ("DBA"); Ernst & Young LLP ("Ernst & Young"); Financial Planning Ass'n ("FPA"); Household Finance Corporation ("Household"); Independent Community Bankers of America ("ICB"); Independent Ins. Agents of America ("Indep. Ins. Agents"); Intuit Inc. ("Intuit"); Information Technology Ass'n of America ("ITAA"); MasterCard International ("MasterCard"); Nat'l Ass'n of Indep. Insurers ("NAII"); Nat'l Ass'n of Mutual Ins. Cos. ("NAMIC"); Nat'l Automotive Dealers Ass'n ("NADA"); Nat'l Retail Federation ("NRF"); Navy Federal Credit Union ("NFCU"); Nat'l Indep. Automobile Dealers Ass'n ("NIADA"); Navy Federal Financial Group ("NFFG"); North American Securities Administrators Ass'n, Inc. ("NASAA"); Ohio Credit Union League ("OCUL"); Oracle Corporation ("Oracle"); Software & Information Industry Ass'n ("SIIA"); Visa USA, Inc. ("Visa").

[10] American Council on Education ("ACE"); Education Finance Council and the National Council of Higher Education Loan Programs; Nat'l Council of Higher Educ. Loan Programs, Inc.; USA Education, Inc. & Student Loan Marketing Ass'n (collectively "Sallie Mae"); Texas Guaranteed Student Loan Corp. ("TGSL"); United Student Aid Funds, Inc. ("USA Funds").

[11] Forest Landreth ("Landreth"); Lou Larson ("Larson"); Sheila Musgrove ("Musgrove"); David Paas ("Paas"); Norman Post ("Post").

[12] Portogo, Inc. ("Portogo"); Tiger Testing; VeriSign, Inc. ("VeriSign").

[13] Equifax, Inc ("Equifax"); Experian Information Solutions, Inc. ("Experian").

[14] Nat'l Ass'n of Consumer Agency Administrators ("NACAA").

[15] *See, e.g.*, Household at 1; Intuit at 2; ITAA at 1; NRF at 2; Sallie Mae at 2; SIIA at 3; TGSL at 1; Verisign at 2.

[16] See, e.g., Visa at 1.

[17] *See, e.g.*, ICB at 2; Musgrove at 2; NADA at 2; NIADA at 9; Paas at 4–6.

[18] Under section 313.3(k)(1) of the Privacy Rule, "financial institution" means: any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). An institution that is significantly engaged in financial activities is a financial institution.

Additional examples of financial institutions are provided in section 313.3(k)(2) of the Privacy Rule.

[19] *See, e.g.*, Equifax at 1–2; Intuit at 2; NIADA at 2; TGSL at 1.

[20] Equifax at 2.

[21] *See, e.g.*, ACA at 2–3; CDIA at 3; Experian at 2; Mastercard at 2–3; NAMIC at 2–3; NRF at 3. In addition, one comment stated that numerous financial institutions that do not have customer relationships of their own could be swept into the Rule in this fashion (Visa at 4). Although no commenters identified the types of financial institutions that are likely to be so affected, the Commission envisions that such entities could include consumer reporting agencies, debt collectors, independent check cashers, automated teller machine operators, and other businesses that obtain customer information from other financial institutions to process customer data, facilitate customer transactions, or carry out transactions in a consumer context.

respect the privacy of these customers and to protect the security and confidentiality of their nonpublic personal information. Covering recipients will ensure that all financial institutions over which the Commission has jurisdiction safeguard customer information and that such safeguards are not lost merely because information is shared with a third-party financial institution.[22] The Commission also believes that the Rule's provisions for affiliates and service providers, discussed below, are not sufficient to address circumstances where information is transferred to another financial institution in the absence of a service or affiliate relationship, such as for use in debt collection or consumer reporting. Without imposing safeguards in such cases, customer information would be insufficiently protected and Congressional intent to safeguard such information would be undermined. Finally, the flexible requirements of the Rule—which allow the safeguards to vary according to the size and complexity of a financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue—permit entities to develop safeguards appropriate to their operations and should minimize any burdens on recipient entities.

Nevertheless, the Commission recognizes that financial institutions covered by its Rule also may simultaneously be subject to the Rule's requirements for service providers or affiliates.[23] For example, check printers, data processors, and real property appraisers that receive customer information as service providers for a financial institution will also be directly subject to the rule because they are themselves financial institutions.[24] However, the obligations the Rule creates for financial institutions are entirely consistent with the standard it requires them to impose on their affiliate or service provider, so that each entity ultimately is required to maintain safeguards that are appropriate in light of the relevant circumstances. Thus, a financial institution that develops an information safeguards program according to the Rule will not be faced with additional or conflicting requirements merely because it also received customer information as an affiliate or service provider.

As under the proposal, the Safeguards Rule does not cover recipients of customer information that are not financial institutions, and are also neither affiliates nor service providers as defined by the Rule. However, the Commission encourages each financial institution to take reasonable steps to assure itself that any third party to which it discloses customer information has safeguards that are adequate to fulfill any representations made by the financial institution regarding the security of customer information or the manner in which it is handled by third parties.[25]

In addition, as under the proposal, the Safeguards Rule only applies to information about a consumer who is a "customer" of a financial institution within the meaning of the Rule.[26] This approach is consistent with the Banking Agency Guidelines and the majority of comments that addressed this issue.[27] Although the Commission believes that limiting the Rule to information about customers is warranted by the plain language of section 501 of the Act, the Commission notes, as it did in the proposal, that protecting information about consumers may be a part of providing reasonable safeguards to "customer information" where the two types of information cannot be segregated reliably. Further, consistent with its mandate under section 5 of the FTC Act, the Commission expects that, as with customers, any information that a financial institution provides to a consumer will be accurate concerning the extent to which safeguards apply to them. Finally, the Commission expects that each financial institution will have in place at least the administrative or other safeguards necessary to honor any "opt-out" requests made by consumers under the Privacy Rule.

Other comments on the Rule's scope urged that compliance with various alternative standards should constitute compliance with the Safeguards Rule. Several such commenters urged that the Rule permit compliance with another agency's safeguards standard in lieu of the FTC's. Specifically, commenters urged that: (1) Compliance with the SEC's rule constitute compliance with the FTC Rule, so that state investment advisors covered by the FTC Rule would be subject to the same standards as federal investment advisors, which are subject to the SEC's jurisdiction;[28] (2) non-federally-insured credit unions be permitted to comply with the NCUA's guidelines instead of the FTC's Rule, so that they would be subject to the same standards as federally-insured credit unions, which are under the NCUA's jurisdiction;[29] and (3) compliance with the Banking Agency Guidelines[30] be deemed compliance for service providers that may be engaged by banks as well as by entities under the FTC's jurisdiction. In addition, other commenters requested that compliance with other laws be deemed compliance with the Rule, such as the Fair Credit Reporting Act ("FCRA");[31] the Health Insurance Portability and Accountability Act ("HIPAA");[32] and the Fair Debt Collection Practices Act ("FDCPA").[33]

As discussed above in connection with recipient financial institutions and others, the Commission does not intend to impose undue burdens on entities that already are subject to comparable safeguards requirements. In particular, the Commission envisions that any entity that can demonstrate compliance with the Banking Agency Guidelines (including the substantively identical NCUA Guidelines) will also satisfy the Rule. With respect to other rules and laws that may contain some safeguards, the Commission notes that the adoption of safeguards in furtherance of such rules or laws will be weighted heavily in assessing compliance with the Rule. However, because such other rules and laws do not necessarily provide comparable protections in terms of the safeguards mandated, data covered, and range of circumstances to which protections apply, compliance with such standards will not automatically ensure compliance with the Rule. For example, an entity's compliance with the FCRA, which limits the purposes for which certain financial information may be disclosed, will not guarantee that an

[22] Under the Act, the Commission has jurisdiction over "any other financial institution or other person that is not subject to the jurisdiction of any agency or authority." 15 U.S.C. Section 6805(7). Thus, the Commission does not have jurisdiction over any financial institution that is subject to another Agency's authority by the Act, including national banks, bank holding companies and savings associations the deposits of which are insured by the FDIC. *See id.* at Section 6805(a)(1)–(6).

[23] As discussed below, the FTC Rule requires financial institutions to ensure the safeguards of their affiliates and take steps to oversee their service providers' safeguards. *See* sections 314.2(b) and 314.4(d), below. What safeguards would be appropriate for an affiliate or service provider depends on the facts and circumstances, just as it would for a financial institution that is directly covered by the Rule.

[24] It should be noted that this potential overlap exists for all financial institutions that are affiliates or service providers of other financial institutions, not just recipient entities.

[25] Misrepresentations regarding these issues could violate the Privacy Rule and Section 5 of the FTC Act.

[26] The Rule incorporates the definition of "customer" set forth in section 313(h) of the Privacy Rule. *See* section 314.2(a).

[27] *See, e.g.*, ACA at 4; DBA at 1; Mastercard at 1–2; *but see* Intuit at 3–4; NACAA at 1.

[28] NASAA at 2.

[29] CUNA at 1; OCUL at 3.

[30] Indep. Ins. Agents at 2.

[31] CDIA at 2–3; NIADA at 3.

[32] NIADA at 3.

[33] ACA at 4–5.

entity has adopted a comprehensive information security plan as described in the Rule.

Section 314.2: Definitions

This section defines terms used in the Safeguards Rule. As under the proposal, paragraph (a) makes clear that, unless otherwise stated, terms used in the Safeguards Rule bear the same meaning as in the Commission's Privacy Rule. The remaining paragraphs (b)-(d) of this section define the terms "customer information," "information security program," and "service provider," respectively.

In addressing this section generally, several commenters expressed concern that the definitions would be confusing to the extent that they differ from those set forth in the Privacy Rule or the Banking Agency Guidelines.[34] In response, the Commission notes that, the terms used in the Rule are consistent with those used in the Privacy Rule, and differ from those used in the Guidelines only as needed to clarify the Rule's scope and make its terms more understandable and appropriate to the diverse range of non-bank financial institutions subject to the Commission's jurisdiction. Thus, as described below, the Rule defines "customer information" to include information handled by affiliates. Similarly, the Rule omits definitions found in the Guidelines, such as "Board of Directors" or "subsidiary," that are not universally applicable to entities that will be subject to the Rule.

Proposed paragraph (b) defined "customer information" as any record containing nonpublic personal information, as defined in paragraph 313.3(n) of the Privacy Rule, about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of a financial institution or its affiliates." Thus, to the extent that a financial institution shares customer information with its affiliates, the proposal required it to ensure that the affiliates maintain appropriate safeguards for the customer information at issue.

Commenters expressed varying views on whether a financial institution should be responsible for its affiliates' safeguards. Some commenters agreed that customer information held by affiliates should be protected by the Rule.[35] However, some commenters requested that affiliates that are financial institutions subject to the jurisdiction of another agency be permitted to comply with the safeguards standards of that agency in lieu of the Commission's Rule.[36] Finally, several commenters stated that the Rule should not cover affiliates at all because (1) the Act was not meant to cover any entity that is not a financial institution and some affiliates may not be financial institutions[37] or (2) the fact that the Act permits financial institutions to disclose nonpublic personal information to affiliates without providing any notice or opt out indicates that no affiliates were intended to be covered by the Act's safeguards provisions.[38]

The Commission agrees that section 501 of the Act focuses on the obligations of financial institutions. It also notes, however, that the purpose of the Act is to protect customer information, and that such information easily may be shared with companies that are affiliated and under common control with such financial institutions. Therefore, the Rule imposes obligations only on financial institutions, but gives them duties with respect to customer information shared with their affiliates. The Commission does not believe that the unrestricted sharing that the Act permits among affiliates—including affiliates that are not financial institutions—shows an intent to exclude affiliates from safeguards obligations. To the contrary, the free sharing the Act permits among affiliates warrants a coordinated and consistent approach to security. The Commission notes, however, that the duty to ensure appropriate safeguards by affiliates arises only if a financial institution shares customer information with its affiliates; therefore this obligation can, and need only be, addressed as part of such sharing arrangements. In addition, the flexible standards of the Rule permit entities to develop safeguards appropriate to their operations and the sensitivity of the information at issue and should therefore minimize burdens on affiliates. Finally, as noted above, the Commission agrees that compliance with the Banking Agency Guidelines should satisfy the safeguards standards under the Commission's Rule. Therefore, any financial institution that can demonstrate its compliance with the Guidelines will not be subject to additional requirements merely because it is an affiliate of a financial institution that is covered by the Rule.

Proposed paragraph (c) defined "information security program" as "the administrative, technical, or physical safeguards" that a financial institution uses "to access, collect, process, store, use, transmit, dispose of, or otherwise handle customer information." This definition is virtually identical to the Banking Agency Guidelines' definition of "customer information systems." *See* Banking Agency Guidelines, section I.C.2.d. Few comments were received on this definition. In response to one commenter who urged that this term should better describe all of the ways that "customer information" can be provided to others, the Commission has added the words "distribute" and "protect" to this definition.[39] At the same time, the Commission notes that the words "otherwise handle" are intended to cover other ways that customer information is dealt with that are not specifically mentioned in the definition. Thus, the definition is adopted with only the minor changes noted above.

Proposed paragraph (d) defined the term "service provider" to mean "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to the rule." This definition is virtually identical to the definition set forth in the Banking Agency Guidelines. *See* Banking Agency Guidelines, section I.C.2.e. Several commenters urged that this definition be amended to exclude particular entities from the definition of service providers, namely: (1) Accountants and auditors[40] (2) financial institutions that also provide services to banks, and are subject to examination under the Bank Service Company Act (BSCA);[41] (3) any service provider that is also an affiliate of a financial institution;[42] and (4) any service provider that receives information under the Privacy Rule's general exceptions in Sections 313.14 and 313.15, and is therefore permitted access to nonpublic personal information without need for a specific agreement concerning its reuse and redisclosure.[43]

The Commission notes that the Banking Agency Guidelines do not contain exceptions to the definition of service provider. Thus, some of the recommended exceptions could result

[34] *See, e.g.*, Intuit at 4; NADA at 2; NIADA at 2, 4.

[35] Equifax at 2–4; Household at 1–2; NACAA at 1; NIADA at 4; SIIA at 2. *See also* NCHELP at 1.

[36] *See, e.g.*, Household at 1–2; NCHELP at 2; OCUL at 2; USA Funds at 1. *See also* Equifax at 2.

[37] Mastercard at 4–5. *See also* NRF at 4.

[38] NAMIC at 5–6.

[39] Equifax at 4.

[40] Ernst & Young at 1–2.

[41] Visa at 4.

[42] NIADA at 5.

[43] NIADA at 6 (but stating that the Rule's obligations for service providers are for the most part consistent with the Privacy Rule).

in disparate treatment of entities performing services for a bank and entities performing services for a financial institution under the FTC's jurisdiction. In addition, no commenters demonstrated that the confidentiality requirements that apply to auditors and accountants (or other professionals) would address unauthorized access to information by third parties, fraud, or any other security issues contemplated by the Rule. Further, given the Rule's flexibility, the Commission is aware of no duplicative burdens that will result from application of the Rule to auditors, accountants, or other professionals, or to service providers to, or affiliates of, banks. Finally, the Commission has determined that the Rule should apply to all service providers, even those that the Privacy Rule does not require to enter into agreements concerning reuse and redisclosure of the relevant information. Although the Privacy Rule allows certain service providers to receive information without entering into confidentiality agreements, these confidentiality provisions do not address the range of security issues that are contemplated by the Safeguards Rule.

Other comments sought minor clarifications of the definition of service provider. Specifically, commenters asked (1) whether a student loan organization is covered where the tasks it performs—passing along updated contact information to schools, lenders, loan servicers, and others involved in the funding of student loans—could not be carried out by financial institutions directly;[44] and (2) whether subservicers, employees and independent contractors of service providers are required to maintain separate safeguards.[45] These concerns are addressed as follows: First, although outsourcing often involves functions that may be performed in-house, the Commission sees no reason to exclude from the Rule service providers that are specifically authorized to perform services that a financial institution cannot perform itself. Thus, such entities are covered to the extent that they meet the definition. Second, the focus of the Rule's service provider provisions is clearly on the original service provider—the entity that provides services "directly to a financial institution"— and not on subservicers or employees or independent contractors of these service providers. Although the original service provider should address the practices of these individuals and entities in its own security plan, the Rule does not specifically require these individual entities to maintain their own safeguards.

For the reasons discussed, the definition of service provider is adopted as proposed.

Section 314.3: Standards for Safeguarding Customer Information

Proposed paragraph (a) of this section set forth the general standard that a financial institution must meet to comply with the Rule, namely to "develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards" that are appropriate to the size and complexity of the entity, the nature and scope of its activities, and the sensitivity of any customer information at issue. This standard is highly flexible, consistent with the comments, the Banking Agency Guidelines, and the Advisory Committee's Report, which concluded that a business should develop "a program that has a continuous life cycle designed to meet the needs of a particular organization or industry."[46] *See* ACR at 18. Paragraph (a) also requires that each information security program include the basic elements set forth in proposed section 314.4 of the Rule, and be reasonably designed to meet the objectives set forth in section 314.3(b). For the reasons discussed below, this standard is adopted with only minor changes.

As noted above, commenters were generally supportive of the proposed standard, citing both its flexibility and its similarity to the Banking Agency Guidelines.[47] In addition, the numerous commenters who addressed whether the information security program should be in writing were supportive of this requirement,[48] stating that such a requirement is reasonable[49] and essential to the effective implementation and management of safeguards.[50] At the same time, two commenters suggested that the term "comprehensive" be deleted to avoid implying that the writing itself should be comprehensive.[51] One commenter urged that the Final Rule explicitly state—as was stated in the section-by-section analysis of the Proposed Rule[52]—that the writing need not be contained in a single document. In response, the Commission has amended the standard slightly, so that each financial institution must "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards" that are appropriate to the size and complexity of the entity, the nature and scope of its activities, and the sensitivity of any customer information at issue. *See* paragraph (a). The Commission believes that this standard will ensure a comprehensive, coordinated approach to security while emphasizing the flexibility of the writing requirement.

One commenter requested that the Rule specify that a financial institution need not disclose its information security plan to any third party other than law enforcers. In response, the Commission notes that the Rule itself creates no obligation for a financial institution to disclose its information security program. Moreover, the Privacy Rule requires a financial institution to disclose to consumers only the most general information about its safeguards. *See* 16 CFR 313.6(a)(8) and (c)(6). However, the Safeguards Rule leaves private parties free to negotiate disclosure of any safeguards information that may be relevant to the business at hand. Further, neither the G–L–B Act nor the Rule provides a shield to disclosure that is sought by law enforcement or pursuant to court order, subpoena or other legal process.

Section 314.4: Elements

This section sets forth the general elements that a financial institution must include in its information security program. The elements create a framework for developing, implementing, and maintaining the required safeguards, but leave each financial institution discretion to tailor its information security program to its own circumstances. Subject to the changes to paragraphs (d) and (e) that are set forth below, these elements are adopted as proposed.

1. Paragraph (a)

Paragraph (a) requires each financial institution to designate an employee or employees to coordinate its information security program in order to ensure accountability and achieve adequate safeguards. This requirement is similar to the Banking Agency Guidelines'

[44] TGSL at 2.

[45] Equifax at 4.

[46] The adaptability of the standard according to "the sensitivity of information" mirrors the Advisory Committee's finding that "different types of data warrant different levels of protection." *Id.*

[47] *See supra* nn.15 and 16, and accompanying text.

[48] CDIA at 4; Equifax at 5; Intuit at 4; NFCU at 1; NFFG at 1; NCHELP at 3; NASAA at 2.

[49] *See, e.g.*, NCHELP at 3.

[50] *See, e.g.*, Intuit at 4.

[51] CDIA at 4; Equifax at 5.

[52] 66 FR at 41165.

requirement that each institution involve and report to its Board of Directors (*see* 66 FR 41166, *citing* Paragraphs III.A. and III.F., respectively), but allows designation of any employee or employees to better accommodate entities that are not controlled by Boards of Directors. Nearly all commenters on this paragraph expressed support, noting the importance of establishing a point of contact and citing the provision's flexibility.[53] However, some commenters requested minor changes, namely: (1) That the Rule state that a financial institution need not designate an employee for each of its subsidiaries; (2) that the words "as appropriate" be added to the requirement; and (3) that the Rule make clear that financial institutions may outsource safeguards procedures.[54] By contrast, one commenter opposed requiring financial institutions to designate any individual employee(s), based on a concern that customers might attempt to hold such designee(s) individually liable for any breach of security that occurs.[55]

The Commission recognizes the importance of reserving to financial institutions the flexibility to select and designate the employee(s) that are needed to ensure accountability and achieve adequate safeguards. The Commission is particularly concerned that small institutions not be burdened disproportionately by this paragraph (or by other requirements) of the Rule. For these reasons, the paragraph allows each financial institution to determine which employee(s) to designate, including whether to designate additional employees to handle different subsidiaries. Further, there is nothing in the Rule to prevent a financial institution from outsourcing safeguards functions as appropriate, provided that at least one of its own employees is designated to see that such functions are properly carried out. At the same time, the Commission declines to add the words "as appropriate" to this paragraph because such language would only repeat the Rule's overarching requirement that each financial institution develop, implement and maintain "appropriate" safeguards. Lastly, the Commission notes that this Rule does not address or alter traditional principles of corporate liability and, therefore, should neither create nor limit individual liability for a financial institution's designated employee(s). Thus, paragraph (a) is adopted as proposed.

2. Paragraph (b)

Proposed paragraph (b) required each financial institution to "identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks." The proposal further required each financial institution to consider risks in each area of its operations, including three areas that the Commission believes are particularly relevant to information security: (1) Employee training and management; (2) information systems, including information processing, storage, transmission and disposal; and (3) detecting, preventing and responding to attacks, intrusions, or other systems failures. This paragraph is similar to the Banking Agency Guidelines requirement to assess risks.[56]

Commenters who addressed the issue generally supported including a risk assessment requirement within the Rule.[57] Some of these commenters supported the paragraph as proposed, stating that its benefits are appropriate relative to its burdens, and that it provides the proper level of guidance on how risk assessment should be carried out.[58] Commenters that supported the paragraph's general description of the types of risks to be considered—including the proposed areas of operation—emphasized that the threats to information security are ever changing, and therefore can only be described in general terms.[59] By contrast, other commenters urged that the paragraph be made more specific in a variety of ways, namely by: (1) Defining specific categories of threats and hazards, such as "risks to physical security;" (2) including more concrete and extensive guidance on how small businesses might perform the required assessment; or (3) including a procedure by which the FTC will conduct reviews or audits of the security practices of financial institutions under its jurisdiction.[60]

The Commission notes the importance of providing guidance to financial institutions, particularly small businesses, on how to comply with this and other aspects of the Rule. The Commission therefore intends to issue educational materials to help businesses identify risks and comply with the various other provisions of the Rule. Because of the ever-changing nature of the relevant risks, however, the Commission does not find it appropriate to delineate risks more specifically within the Rule. In addition, to retain appropriate flexibility, the Commission will rely on its discretion in enforcing the Rule, and not describe any particular schedule or methods for enforcement.[61] At the same time, the Commission has amended slightly the areas of operation, in order to better describe the activities that financial institutions should consider in developing, implementing and maintaining their information security programs. Specifically, the Commission has added (1) the item "network and software design" to the examples of information systems a financial institution should examine; and (2) the term "detecting" to the requirement that each financial institution consider means of "preventing and responding" to attacks, intrusions and other systems failures. In all other respects, paragraph (b) is adopted as proposed.

3. Paragraph (c)

Proposed paragraph (c) required each financial institution to "design and implement information safeguards to control the risks [identified] through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures." The proposal further required each financial institution to consider its areas of operation in fulfilling this requirement. As with proposed paragraph (b), above, commenters generally supported this provision, citing its flexibility and the appropriateness of its benefits relative to its burdens.[62] However, one commenter

[53] *See, e.g.*, Intuit at 4; Mastercard at 6–7; NACAA at 1–2; NCHELP at 3; Sallie Mae at 3; SIIA at 2; Visa at 2.

[54] Sallie Mae at 3; Equifax at 6; NRF at 5, respectively.

[55] NIADA at 6.

[56] *See* Banking Agency Guidelines, Paragraph III. B.

[57] *See, e.g.*, Equifax at 7; Intuit at 5; Mastercard at 7; NASAA at 2; NCHELP at 3; Portogo at 1; SIAA at 4; VeriSign at 1.

[58] *See, e.g.*, Intuit at 5; Mastercard at 7; SIAA at 2.

[59] Oracle at 2; Mastercard at 7.

[60] NACAA comment on the ANPR, at 2; Paas at 3; Musgrove at 2, respectively.

[61] By contrast to the Banking Agencies, the Commission is not authorized to conduct regular audits and review of entities under its jurisdiction.

[62] Intuit at 5; NCHELP at 4; SIIA at 2. In addition, as elsewhere, commenters urged that the paragraph include more guidance, so that businesses—particularly smaller entities, such as sole proprietorships—will better understand what safeguards are sufficient to comply with the Rule. *See* NIADA at 7–8; Paas at 4–5. As discussed above, the Commission agrees that educating businesses

Continued

asked that the provision be revised to require only such safeguards as are "commercially reasonable," [63] while another urged that the paragraph require each financial institution to keep specific written records of its particular safeguards procedures, such as its employee training activities and records retention schedules, to demonstrate compliance with the Rule.[64]

The Commission recognizes that each financial institution must focus its limited resources on addressing those risks that are most relevant to its operations. However, because the Rule already contains flexible standards that take a variety of factors into account, the Commission does not believe it is necessary or appropriate to revise the Rule to require only such safeguards as are "commercially reasonable." At the same time, to preserve flexibility and minimize burdens, the Commission declines to revise this paragraph to require that financial institutions document specific aspects of their risk control activities. For these reasons, paragraph (c) is adopted as proposed.

4. Paragraph (d)

Proposed paragraph (d) required each financial institution to oversee its service providers by selecting and retaining service providers that are "capable of maintaining appropriate safeguards" for the customer information at issue (paragraph (d)(1)), and requiring its service providers by contract to "implement and maintain such safeguards" (paragraph(d)(2)). For the reasons discussed below, paragraph (d)(1) is revised slightly, while paragraph (d)(2) is adopted as proposed.

Commenters supported requiring oversight of service providers' safeguards by financial institutions, particularly when, as one coalition of financial services organizations noted, the financial services industry increasingly relies on third parties to support core functions and online delivery.[65] However, in commenting on proposed paragraph (d)(1), some commenters expressed concern about the ability of businesses—particularly smaller entities—to evaluate a service provider's capabilities.[66] At the same time, other commenters supported adding to the Rule various standards for financial institutions to use in selecting service providers, specifically: (1) That financial institutions have "reason to believe" their service providers are capable of maintaining appropriate safeguards; [67] (2) that they use a "due diligence" review, as under the Banking Agency guidelines; [68] or (3) that they select service providers that are "capable of maintaining appropriate safeguards." [69]

The Commission agrees that businesses cannot be expected to perform unlimited evaluation of their service providers' capabilities. Thus, the Commission has amended the provision to state that each financial institution must "take reasonable steps" to select and retain appropriate service providers. This added language more closely parallels the Banking Agency Guidelines, as well as the Rule's requirement to assess risks that are "reasonably foreseeable." The steps that are reasonable under the Rule will depend upon the circumstances and the relationship between the financial institution and the service provider in question. At a minimum, the Commission envisions that each financial institution will (1) take reasonable steps to assure itself that its current and potential service providers maintain sufficient procedures to detect and respond to security breaches, and (2) maintain reasonable procedures to discover and respond to widely-known security failures by its current and potential service providers.

Proposed paragraph (d)(2) required financial institutions to enter into contracts that require service providers to implement and maintain appropriate safeguards. Most comments that addressed this requirement supported it.[70] Nevertheless, as discussed above, some commenters urged that certain service providers be exempt from the Rule, or be permitted to comply with the safeguards standards of another agency, such as their own functional regulator in the case of financial institution service providers. These comments already have been addressed above. In addition, two commenters urged that the Rule give examples of appropriate language or specifically require the inclusion of certain clauses in the contract,[71] while other commenters stated that no such specifications are needed or desirable.[72] The Commission believes that financial institutions are well positioned to develop and implement appropriate contracts with their service providers. Further, keeping the contract provision flexible should allow financial institutions and their service providers to develop arrangements that do not impose undue or conflicting burdens on service providers that may be subject to other standards and/or agreements concerning safeguards. Therefore, the Commission declines to include specific contract language within the Rule. However, the Commission intends to provide education for businesses on how to comply with the Rule, and will include general guidance concerning oversight of service providers as part of this effort. For these reasons, paragraph (d)(2) is adopted as proposed.

5. Paragraph (e)

Proposed paragraph (e) required each financial institution to "evaluate and adjust [its] information security program in light of any material changes to [its] business that may affect [its] safeguards." The preamble to the proposed section offered examples of such material changes, namely changes in technology; changes to its operations or business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, or changes to the services provided; new or emerging internal or external threats to information security; or any other circumstances that give it reason to know that its information security program is vulnerable to attack or compromise. *See* 66 FR 41167. Several commenters supported this requirement as proposed.[73] However, a few commenters recommended certain revisions to the paragraph's description of the types of changes that may warrant evaluation and adjustment of an entity's safeguards. Specifically, one commenter urged that although changes in the sensitivity of customer information or the nature of any threats will warrant evaluation, changes to a business's internal organization may be irrelevant to its safeguards, and therefore should not necessitate a review.[74] Similarly, another commenter urged that the paragraph be revised to require that a financial institution "take reasonable steps so that the information security

and others is critical to achieving the Rule's objectives, and plans to issue educational materials in connection with the Rule.

[63] Equifax at 8.

[64] Musgrove at 2.

[65] BITS at 1. *See also* CDIA at 6; ITAA at 3; VeriSign at 2 (Rule appropriately places on financial institutions the burden to select appropriate service providers).

[66] Paas at 5. *See also* NRF at 5 (expressing concern that Rule could make financial institutions strictly liable for safeguards breaches by their service providers).

[67] NRF at 5; TGSL at 2.

[68] Household at 1; ICBA at 1; NIADA at 6.

[69] Mastercard at 7.

[70] Equifax at 8; Indep. Ins. Agents 3; Intuit at 5; Mastercard at 7; NACAA at 2; NCHELP at 4; Navy Federal Financial Group at 1–2; NIADA at 7; Sallie Mae at 3; SIIA at 2.

[71] NADA at 3; Navy Federal Financial Group at 1–2.

[72] Intuit at 5; Sallie Mae at 3.

[73] NACAA at 2; NCHELP at 5; SIIA at 2.

[74] Intuit at 6.

program continues to be appropriate" for the financial institution.[75]

Consistent with the intent of the Proposed Rule, as well as the concerns reflected in these comments, the Commission believes that the bases for a financial institution to adjust its information security program will vary depending on the circumstances and may include a wide range of factors. Accordingly, paragraph (e) has been amended to more clearly reflect the fact-specific nature of the inquiry and to better encompass the broad range of factors that a financial institution should consider. Under the revised paragraph, each financial institution must evaluate and adjust its information security program "in light of the results of the testing and monitoring required by paragraph (c); any material changes to [its] operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on [its] information security program." The Commission believes that the Rule allows a financial institution sufficient flexibility as to how to adjust its safeguards, and therefore finds it unnecessary to limit the responsibility of financial institutions to taking "reasonable steps" to make any adjustments. Thus, paragraph (e) is adopted with the changes noted above.

Section 314.5: Effective Date

Proposed section 314.5 required each financial institution covered by the Rule to implement an information security program not later than one year from the date on which a Final Rule is issued. In addition, the proposal requested comment on whether the Rule should contain a transition period to allow the continuation of existing contracts with service providers, even if the contracts would not satisfy the Rule's requirements.

Many commenters supported as adequate an effective date of one year from the date on which the Final Rule is issued.[76] A few commenters urged that a longer time be given, such as 18 months,[77] or that an additional year be allowed for businesses—particularly small entities—to comply.[78] In addition, all commenters who addressed the issue urged that the Rule allow a transition period for service provider contracts.[79] Most of these commenters requested that financial institutions be given two years to make service provider contracts comply,[80] while a few commenters sought a slightly longer time.[81]

Consistent with the majority of comments, the Rule will take effect one year from the date on which the Final Rule is published in the **Federal Register**, except that there will be a transition rule for contracts between financial institutions and nonaffiliated third party service providers. Under the transition Rule, set forth in section 314.5(b) of the Rule, financial institutions will be given an additional year to bring these service provider contracts into compliance with the Rule, as long as the contract was in place 30 days after the date on which the Final Rule is published in the **Federal Register**. The transition rule parallels the two-year grandfathering of service contracts that was permitted under both the Privacy Rule and the Banking Agency Guidelines. The Commission believes that the effective date and transition rule will provide businesses appropriate flexibility in complying with the Rule.

Section D. Paperwork Reduction Act

The Paperwork Reduction Act ("PRA"), 44 U.S.C. Chapter 35, requires federal agencies to seek and obtain OMB approval before undertaking a collection of information directed to ten or more persons. 44 U.S.C. 3502(3)(a)(i). Under the PRA, a rule creates a "collection of information" where ten or more persons are asked to report, provide, disclose, or record information" in response to "identical questions." *See* 44 U.S.C. 3502(3)(A). Applying these standards, the Rule does not constitute a "collection of information." The Rule calls upon affected financial institutions to develop or strengthen their information security programs in order to provide reasonable safeguards. Under the Rule, each financial institution's safeguards will vary according to its size and complexity, the nature and scope of its activities, and the sensitivity of the information involved. For example, a financial institution with numerous employees would develop and implement employee training and management procedures beyond those that would be appropriate or reasonable for a sole proprietorship, such as an individual tax preparer or mortgage broker. Similarly, a financial institution that shares customer information with numerous affiliates would need to take steps to ensure that such information remains protected, while a financial institution with no affiliates would not need to address this issue. Thus, although each financial institution must summarize its compliance efforts in one or more written documents, the discretionary balancing of factors and circumstances that the Rule allows—including the myriad operational differences among businesses that it contemplated—does not require entities to answer "identical questions," and therefore does not trigger the PRA's requirements. *See* "The Paperwork Reduction Act of 1995: Implementing Guidance for OMB Review of Agency Information Collection," Office of Information and Regulatory Affairs, OMB (August 16, 1999), at 20–21.

Section E. Regulatory Flexibility Act

In its ANPR, the Commission stated its belief that, under the Regulatory Flexibility Act ("RFA"), 5 U.S.C. 604(a), it was not required to issue an Initial Regulatory Flexibility Analysis ("IRFA") because the Commission did not expect that the Proposed Rule would have a significant economic impact on a substantial number of small entities within the meaning of the Act. *See* 66 FR at 41167. The Commission nonetheless issued an IRFA with the Proposed Rule in order to inquire into the possible impact of the Proposed Rule on small entities, and to provide information to small businesses, as well as other businesses, on how to implement the Rule. *Id.*

Although the Commission specifically sought comment on the costs to small entities of complying with the Rule, no commenters provided specific cost information. Some commenters generally praised the proposal's flexibility[82] or noted that given its flexible standards, it was appropriate for the Rule to apply equally to businesses of all sizes.[83] However, other commenters suggested that small entities may be disproportionately burdened by the Rule because they lack expertise (relative to larger entities) in developing, implementing and maintaining the required safeguards.[84] In light of these comments, the Commission has carefully considered whether to certify that the Rule will not have a significant impact on a

[75] Equifax at 9.

[76] *See, e.g.*, Equifax at 10; Intuit at 6; Mastercard at 8; NIADA at 8; OCUL at 3; Sallie Mae at 3; SIIA at 2; USA Funds at 1–2.

[77] NADA at 2–3; NIADA at 8. *See also* NFFG at 2 (2 years).

[78] ACA at 6–7.

[79] *See, e.g.*, CDIA at 5; NIADA at 8; OCUL at 3; SIIA at 2; TGSL at 2; Visa at 5.

[80] *See, e.g.*, Equifax at 10; NRF at 5; NFFG at 2; OCUL at 3.

[81] Sallie Mae at 3; Visa at 5.

[82] *See, e.g.*, Household at 1; SIIA at 1; TGSL at 1; VeriSign at 1.

[83] Intuit at 2; NASAA at 2.

[84] *See, e.g.*, NADA at 2; NIADA at 9; Musgrove at 2 (stating that small financial institutions may need to hire outside consultants to comply with Rule).

substantial number of small entities. The Commission continues to believe that the Rule's impact will not be substantial in the case of most small entities. However, the Commission cannot quantify the impact the Rule will have on such entities. Therefore, in the interest of thoroughness, the Commission has prepared the following Final Regulatory Flexibility Analysis ("FRFA") with this Final Rule. 5 U.S.C. 605.

1. Succinct Statement of the Need for, and Objectives of, the Rule

The Final Rule is necessary in order to implement section 501(b) of the G–L–B Act, which requires the FTC to establish standards for financial institutions subject to its jurisdiction relating to administrative, technical, and physical standards. According to section 501(b), these standards must: (1) Insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. These objectives have been discussed above in the statement of basis and purpose for the Final Rule.

2. Summary of the Significant Issues Raised by the Public Comments in Response to the IRFA; Summary of the Assessment of the Agency of Such Issues; and Statement of Any Changes Made in the Rule as a Result of Such Comments

As stated above, no comments were received concerning specific costs that will be imposed on small entities by the Rule. However, some commenters stated that the Rule and/or certain of its requirements would impose high costs on businesses, including small entities.[85] In addition, as stated, a few commenters suggested that small entities may be disproportionately burdened by the Rule because they lack expertise (relative to larger entities) in developing, implementing and maintaining the required safeguards.[86] Finally, as stated above, many commenters urged that the Commission provide guidance on how to comply with the Rule to assist entities—particularly smaller businesses—to comply without incurring undue expense.[87] In addition, some commenters specifically requested guidance on how to assess risks as required by section 314.4(b);[88] develop, implement and maintain safeguards as required by section 314.4(c); [89] and oversee service providers as required by section 314.4(d).

The Commission took comments respecting the Rule's impact on small entities into account by designing flexible safeguards standards (section 313.3(a)). Similarly, the Commission took smaller entities into account in allowing each financial institution to decide for itself what employees to designate to handle safeguards (section 314.4(a)), in order to give businesses, particularly smaller entities, flexibility in complying with the Rule. Lastly, because some commenters expressed concern about the ability of businesses—particularly smaller entities—to evaluate a service provider's capabilities,[90] the Commission amended the relevant paragraph to state that each financial institution must "take reasonable steps" to select and retain appropriate service providers.

In addition to the above changes, the Commission has taken into account those comments that stated the importance of educating businesses and others on how to implement and maintain information safeguards. The Commission agrees that such education is critical to achieving the Rule's objectives and to minimizing burdens on businesses. Thus, as stated in the Rule's preamble, the Commission plans to provide educational materials on or near the date on which compliance is required. As part of this effort, the Commission intends to perform outreach to inform small entities, such as individual tax preparers or other sole proprietors, of the Rule and its requirements.

In addition to the forthcoming educational materials, the Commission has given guidance in the Rule and its Preamble that is intended to assist businesses, particularly small entities, to comply with the Rule. Specifically, as discussed above, the Commission has included within the Rule a brief description of those areas of a business' operations that the Commission believes are most relevant to information security: (1) Employee training and management; (2) information systems, including network and software design, as well as information processing, storage, transmission and disposal; and (3) detecting, preventing and responding to attacks, intrusions, or other systems failures. *See* section 314.3(b).

3. Description and Estimate of the Number of Small Entities to Which the Rule Will Apply or an Explanation of Why No Such Estimate Is Available

As previously discussed in the IRFA accompanying the Proposed Rule, it is difficult to estimate accurately the number of small entities that are financial institutions subject to the Rule. The definition of "financial institution," as under the Privacy Rule, includes any institution the business of which is engaging in a financial activity, as described in section 4(k) of the Bank Holding Company Act, which incorporates by reference the activities listed in 12 CFR 225.28 and 12 CFR 211.5(d), consolidated in 12 CFR 225.86. *See* 65 FR 14433 (Mar. 17, 2000).

The G–L–B Act does not specify the categories of financial institutions subject to the Commission's jurisdiction; rather, section 505(a)(5) vests the Commission with enforcement authority with respect to "any other financial institution or other person that is not subject to the jurisdiction of any [other] agency or authority [charged with enforcing the statute]." Financial institutions covered by the Rule will include many of the same lenders, financial advisors, loan brokers and servicers, collection agencies, financial advisors, tax preparers, real estate settlement services, and others that are subject to the Privacy Rule. Many of these financial institutions will not be subject to the Safeguards Rule to the extent that they do not have any "customer information" within the meaning of the Safeguards Rule. The Commission did not receive comments that helped it to identify in any comprehensive manner the small entities that will be affected by the rule. However, one commenter, the National Association of Automobile Dealers Association ("NADA") submitted 1999 data showing that, at that time, 5,292 franchised new automobile dealers had 30 or fewer employees; 1,706 had 20 or fewer employees; and 575 had 10 or fewer employees.[91] In addition, the Commission is aware that many small businesses, such as individual tax preparers or mortgage brokers, will be covered by the Rule.

[85] FPA at 3; Paas at 2; *see also* OCUL (stating that the NCUA's safeguards rule is very burdensome for credit unions); Post at 1 (stating that Privacy Rule is very burdensome).

[86] *See supra* n. 81.

[87] *See, e.g.*, ICB at 2; Musgrove at 2; NADA at 2; NIADA at 9; Paas at 4–6.

[88] Paas at 3.

[89] *See* NIADA at 7; Paas at 4–5.

[90] Paas at 5; *see also* NRF at 5 (expressing concern that Rule could make financial institutions strictly liable for safeguards breaches by their service providers).

[91] NADA at 1.

4. Description of the Projected Reporting, Recordkeeping and Other Compliance Requirements of the Rule, Including an Estimate of the Classes of Small Entities That Will Be Subject to the Requirement and the Type of Professional Skills Necessary for Preparation of the Report or Record

As explained in the Commission's IRFA and the Paperwork Reduction Act discussion that appears elsewhere in this document, the Safeguards Rule does not impose any specific reporting or recordkeeping requirements. Accordingly, compliance with the Rule does not entail expenditures for particular types of professional skills that might be needed for the preparation of such reports or records.

The Rule, however, requires each covered institution to develop a written information security program covering customer information that is appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue. The institution must designate an employee or employees to coordinate its safeguards; identify reasonably foreseeable risks and assess the effectiveness of any existing safeguards for controlling these risks; design and implement a safeguards program and regularly monitor its effectiveness; require service providers (by contract) to implement appropriate safeguards for the customer information at issue; and evaluate and adjust its program to material changes that may affect its safeguards, such as new or emerging threats to information security. As discussed above, these requirements will apply to institutions of all sizes that are subject to the FTC's jurisdiction pursuant to the Rule, including small entities, although the Commission did not receive comments that would enable a reliable estimate of the number of such small entities.

In light of concerns that compliance with these requirements might require the use of professional consulting skills that could be costly, the Commission, as explained in its IRFA, fashioned the Rule's requirements to be as flexible as possible consistent with the purposes of the G–L–B Act, so that entities subject to the Rule, including small entities, could simplify their information security program to the same extent that their overall operations are simplified. Furthermore, the Commission invited comments on the costs of establishing and operating an information security program for such entities, particularly any costs stemming from the proposed requirements to: (1) Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, and (2) develop a comprehensive information security program in written form. In response to comments that raised concerns that many businesses would not possess the required resources or expertise to fulfill the Rule's requirements, the Commission notes that the Rule is not intended to require that entities hire outside experts or consultants in order to comply. Further, the Commission has noted that it intends to provide educational materials that will assist such entities in compliance. In addition, in response to concerns that the preparation of a written plan could be burdensome, the Commission amended this requirement slightly to emphasize the flexibility of the writing requirement and make clear that the writing need not be contained in a single document.

5. Description of the Steps the Agency Has Taken To Minimize the Significant Economic Impact on Small Entities, Consistent with the Stated Objectives of Applicable Statutes, Including a Statement of the Factual, Policy, and Legal Reasons for Selecting the Alternative Adopted in the Final Rule and Why Each of the Other Significant Alternatives to the Rule Considered by the Agency That Affect the Impact on Small Entities Was Rejected

The G–L–B Act requires the FTC to issue a rule that establishes standards for safeguarding customer information. The G–L–B Act requires that standards be developed for institutions of all sizes. Therefore, the Rule applies equally to entities with assets of $100 million or less, and not just to larger entities.

As previously noted, the Commission does not believe the Safeguards Rule imposes a significant economic impact on a substantial number of small entities. Nonetheless, to the extent that small entities are subject to the Rule, it imposes flexible standards that allow each institution to develop an information security program that is appropriate to its size and the nature of its operations. In this way, the impact of the Rule on small entities and any other entities subject to the Rule is no greater than necessary to effectuate the purposes and objectives of the G–L–B Act, which requires that the Commission adopt a rule specifying procedures sufficient to safeguard the privacy of customer information protected under the Act. To the extent that commenters suggested alternative regulatory approaches—such as that compliance with alternative standards be deemed compliance with the Rule—that could affect the Rule's impact on small entities, those comments and the Commission's responses are discussed above in the statement of basis and purpose for the Final Rule.

List of Subjects for 16 CFR Part 314

Consumer protection, Credit, Data protection, Privacy, Trade practices.

Final Rule

For the reasons set forth in the preamble, the Federal Trade Commission amends 16 CFR chapter I, subchapter C, by adding a new part 314 to read as follows:

PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Sec.

Authority: 15 U.S.C. 6801(b), 6805(b)(2).

§ 314.1 Purpose and scope.

(a) *Purpose.* This part, which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

(b) *Scope.* This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission ("FTC" or "Commission") has jurisdiction. This part refers to such entities as "you." This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

§ 314.2 Definitions.

(a) *In general.* Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Commission's rule governing the Privacy of Consumer Financial Information, 16 CFR part 313.

(b) *Customer information* means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

(c) *Information security program* means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

(d) *Service provider* means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.

§ 314.3 Standards for safeguarding customer information.

(a) *Information security program.* You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) *Objectives.* The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure the security and confidentiality of customer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

§ 314.5 Effective date.

(a) Each financial institution subject to the Commission's jurisdiction must implement an information security program pursuant to this part no later than May 23, 2003.

(b) Two-year grandfathering of service contracts. Until May 24, 2004, a contract you have entered into with a nonaffiliated third party to perform services for you or functions on your behalf satisfies the provisions of § 314.4(d), even if the contract does not include a requirement that the service provider maintain appropriate safeguards, as long as you entered into the contract not later than June 24, 2002.

By direction of the Commission.

Donald S. Clark,

Secretary.

[FR Doc. 02–12952 Filed 5–22–02; 8:45 am]

BILLING CODE 6750–01–P

U.S.Department of Health & Human Services

Medical Privacy - National Standards to Protect the Privacy of Personal Health Information

SAMPLE BUSINESS ASSOCIATE CONTRACT PROVISIONS

(Published in FR 67 No.157 pg.53182, 53264 (August 14, 2002))

Statement of Intent

The Department provides these sample business associate contract provisions in response to numerous requests for guidance. This is only sample language. These provisions are designed to help covered entities more easily comply with the business associate contract requirements of the Privacy Rule. However, use of these sample provisions is not required for compliance with the Privacy Rule. The language may be amended to more accurately reflect business arrangements between the covered entity and the business associate.

These or similar provisions may be incorporated into an agreement for the provision of services between the entities or they may be incorporated into a separate business associate agreement. These provisions only address concepts and requirements set forth in the Privacy Rule and alone are not sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this sample is not sufficient for compliance with State law and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Furthermore, a covered entity may want to include other provisions that are related to the Privacy Rule but that are not required by the Privacy Rule. For example, a covered entity may want to add provisions in a business associate contract in order for the covered entity to be able to rely on the business associate to help the covered entity meet its obligations under the Privacy Rule. In addition, there may be permissible uses or disclosures by a business associate that are not specifically addressed in these sample provisions, for example having a business associate create a limited data set. These and other types of issues will need to be worked out between the parties.

Sample Business Associate Contract Provisions[1]

Definitions (alternative approaches)
Catch-all definition:

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule.

Examples of specific definitions:

@. Business Associate. "Business Associate" shall mean [Insert Name of Business Associate].

a. Covered Entity. "Covered Entity" shall mean [Insert Name of Covered Entity].

b. Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

c. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

d. Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR § 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

e. Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.501.

f. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

Obligations and Activities of Business Associate

@. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.
a. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
b. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

[This provision may be included if it is appropriate for the Covered Entity to pass on its duty to mitigate damages to a Business Associate.]

c. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

d. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

e. Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner [Insert negotiated terms], to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524. [Not necessary if business associate does not have protected health information in a designated record set.]

f. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual, and in the time and manner [Insert negotiated terms]. [Not necessary if business associate does not have protected health information in a designated record set.]

g. Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available [to the Covered Entity, or] to the Secretary, in a time and manner [Insert negotiated terms] or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

h. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

i. Business Associate agrees to provide to Covered Entity or an Individual, in time and manner [Insert negotiated terms], information collected in accordance with Section [Insert Section Number in Contract Where Provision (i) Appears] of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

Permitted Uses and Disclosures by Business Associate

General Use and Disclosure Provisions [(a) and (b) are alternative approaches]

@. Specify purposes:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity:
[List Purposes].

a. Refer to underlying services agreement:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [Insert Name of Services Agreement], provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

Specific Use and Disclosure Provisions [only necessary if parties wish to allow Business Associate to engage in such activities]

@. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
a. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
b. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 CFR § 164.504(e)(2)(i)(B).
c. Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with § 164.502(j)(1).

Obligations of Covered Entity

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions [provisions dependent on business arrangement]

@. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.
a. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.
b. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. [Include an exception if the Business Associate will use or disclose protected health information for, and the contract includes provisions for, data aggregation or management and administrative activities of Business Associate].

Term and Termination

@. Term. The Term of this Agreement shall be effective as of [Insert Effective Date], and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section. [Term may differ.]

a. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement [and the _____ Agreement/ sections ____ of the _____ Agreement] if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;
2. Immediately terminate this Agreement [and the _____ Agreement/ sections ____ of the _____ Agreement] if Business Associate has breached a material term of this Agreement and cure is not possible; or

3. If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary.

[Bracketed language in this provision may be necessary if there is an underlying services agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]

b. Effect of Termination.

1. Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.
2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon [Insert negotiated terms] that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Miscellaneous

@. Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

a. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

b. Survival. The respective rights and obligations of Business Associate under Section [Insert Section Number Related to "Effect of Termination"] of this Agreement shall survive the termination of this Agreement.

c. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

1 Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions and are not intended to be included in the contractual provisions.

Federal Register

Wednesday,
May 24, 2000

Part III

Federal Trade Commission

16 CFR Part 313
Privacy of Consumer Financial Information; Final Rule

FEDERAL TRADE COMMISSION

16 CFR Part 313

Privacy of Consumer Financial Information

AGENCY: Federal Trade Commission.

ACTION: Final Rule.

SUMMARY: The Federal Trade Commission (the ''Commission'' or ''FTC'') is publishing a final privacy rule, as required by section 504(a) of the Gramm-Leach-Bliley Act, Pub. L. 106-102 (the ''G-L-B Act'' or ''Act''), with respect to financial institutions and other persons under the Commission's jurisdiction, as set forth in section 505(a)(7) of the Act. Section 504 of the Act requires the Commission and other federal regulatory agencies to issue regulations as may be necessary to implement notice requirements and restrictions on a financial institution's ability to disclose nonpublic personal information about consumers to nonaffiliated third parties. Pursuant to section 503 of the G-L-B Act, a financial institution must provide its customers with a notice of its privacy policies and practices. Section 502 prohibits a financial institution from disclosing nonpublic personal information about a consumer to nonaffiliated third parties unless the institution satisfies various disclosure and opt-out requirements and the consumer has not elected to opt out of the disclosure. This final rule implements the requirements outlined above.

EFFECTIVE DATE: This rule is effective November 13, 2000. Full compliance is required by July 1, 2001.

FOR FURTHER INFORMATION CONTACT: Kellie A. Cosgrove or Clarke Brinckerhoff, Attorneys, Division of Financial Practices, Federal Trade Commission, Washington, DC 20580, 202–326–3224.

SUPPLEMENTARY INFORMATION:

Section A. Background

On November 12, 1999, President Clinton signed the G-L-B Act (Public Law 106–102) into law. Subtitle A of Title V of the Act, captioned Disclosure of Nonpublic Personal Information, limits the instances in which a financial institution may disclose nonpublic personal information about a consumer to nonaffiliated third parties, and requires a financial institution to disclose to all of its customers the institution's privacy policies and practices with respect to information sharing with both affiliates and nonaffiliated third parties. The Commission notes that there are other laws that may impose limitations on disclosures of nonpublic personal information in addition to those imposed by the G-L-B Act and this rule. For instance, the Fair Credit Reporting Act imposes conditions on the sharing of application information and credit report information between affiliates and nonaffiliated third parties.[1] Title V also requires the Commission, along with the Federal banking agencies [2] and other Federal regulatory authorities,[3] after consulting with representatives of State insurance authorities designated by the National Association of Insurance Commissioners (NAIC), to prescribe such regulations as may be necessary to carry out the purposes of the provisions in Title V, Subtitle A, that govern disclosure of nonpublic personal information. The Federal agencies are sometimes referred to collectively in this document as the ''Agencies'' (or ''other Agencies'' when excluding the Commission).

The Agencies are all issuing final rules to implement Subtitle A that are consistent and comparable to the extent possible, as is required by the statute.

Section B. Overview of Comments Received

On March 1, 2000, the Commission published a notice of proposed rulemaking (the proposal or proposed rule) in the **Federal Register** (65 FR 11174). The other Agencies published their proposed rules on different dates.[4] The Commission received a total of 640 comments, and the other Agencies collectively received a total of 8,337 comments in response to the various proposed rules. Many commenters sent the same letter to multiple Agencies. Many of the comments were from individuals, virtually all of whom encouraged the Agencies to provide greater protection of individuals' financial privacy. Many individuals noted their concerns generally about the loss of privacy and the receipt of unwanted solicitations by marketers. A large number of individuals also requested the Agencies to support legislation that the commenters believe would provide additional protections.

The Agencies also received several letters from members of Congress. In two letters signed by several members of the House of Representatives, the Agencies were encouraged to exercise their rulemaking authority to provide greater protections than provided in the Act. Other Representatives requested, in separate letters, that some other Agencies (a) create a limited exception to the prohibition against the sharing of account numbers for marketing purposes and (b) ensure that social security numbers are considered ''nonpublic personal information.''

The NAIC submitted a comment on behalf of the State insurance authorities that generally supported the Agencies' proposed rule. The NAIC also proposed various measures to provide greater protections for consumers, such as specifying more convenient means to exercise the right to opt out of the disclosure of information. The NAIC further advised the Agencies to clarify the boundary of Federal and State jurisdiction over privacy regulations and ensure that the financial privacy rules under the Act are compatible with the privacy rules relating to medical information that are to be issued by the Secretary of the Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act (HIPPA) of 1996.[5]

Other comments were received from consumer groups and others advocating that the Agencies extend privacy protections in a number of ways, such as by requiring (a) financial institutions to provide consumers with access to their information maintained by the institutions and the opportunity to correct errors, (b) more detailed disclosures of the information collected and disclosed, and (c) disclosures of a financial institution's privacy policies and practices earlier in the process of establishing a customer relationship. A letter signed by 33 State Attorneys General urged some other Agencies to add certain consumer protections to the disclosure requirements and to the

[1] The Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681 *et seq*, provides no limitation on communication by an entity solely of its own ''transactions or experiences'' with the consumer (*e.g.*, the individual's account history). However, it limits the reporting of information obtained from other sources, such as consumer application information or credit report information. An institution may normally share such data with its affiliates only if it has complied with the notice and opt-out procedures set forth in FCRA § 603(d)(2)(A)(iii), which are very similar to those set forth in Section 502(b)(1) of the Act. Sharing such data with nonaffiliates may be effectively prohibited by the FCRA, because the institution likely would become a consumer reporting agency subject to its restrictions on reporting of information to third parties.

[2] Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (FRB), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), and Secretary of the Treasury.

[3] National Credit Union Administration (NCUA) and Securities and Exchange Commission (SEC).

[4] Those proposed rules, which were consistent and comparable with the proposals published by the Commission, appeared in the **Federal Register** at 65 FR 8770 (Feb. 22, 2000) (OCC, FRB, FDIC, and OTS jointly), 65 FR 10988 (Mar. 1, 2000) (NCUA), and 65 FR 12354 (Mar. 8, 2000) (SEC).

[5] These proposed regulations were published for comment at 64 FR 59918 (Nov. 3, 1999).

provision permitting financial institutions to enter into joint marketing agreements.

Most of the remaining comments were from businesses concerned about the Act, and their representatives. This included not only creditors of various types, but also representatives of the health care industry, retail merchants, insurance companies, securities firms, private investigators, debt collection agencies, consumer reporting agencies, institutions of higher education, tax professionals, and others. These commenters offered a large number of suggested changes, with the most commonly advanced suggestions including: an extension of the effective date of the rule; an amendment to the definition of ''nonpublic personal information'' to focus more narrowly on ''financial'' information; a streamlining of information required in the initial and annual disclosures; a clarification of how one or more of the statutory exceptions operate; an exclusion from, or clarification of, the definitions of ''consumer'' and ''customer'' in various contexts; and the addition of flexibility to provide initial notices at some point other than ''prior to'' the time a customer relationship is established.

The Commission has made some modifications to its proposed rule in light of the comments received. These comments, and the Commission's responses thereto, are discussed in the following section-by-section analysis. Following the section-by-section analysis, the Commission has provided guidance for certain institutions in order to provide additional direction on how these institutions may comply with the rule and avoid unnecessary burden.

Section C. Section-by-Section Analysis

As an initial matter, the Commission notes that the final rule, unlike the proposal, presents the various sections in subparts that consist of related sections. This change was made to group related concepts together and thereby make the rule easier to follow. A derivation table is included following this preamble to assist readers in locating provisions as set out in the Commission proposal. The Commission has also added an Appendix to the final rule, setting out example disclosure clauses for financial institutions to consider.

Section 313.1 Purpose and Scope

Purpose. Paragraph (a) of this section states that the rule is intended to require a financial institution to provide notice to customers about its privacy policies and practices; to describe the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and to provide a method for consumers to prevent a financial institution from disclosing that information to certain nonaffiliated third parties by ''opting out'' of that disclosure, subject to various exceptions as stated in the rule. No significant comments addressed this provision, and the Commission made no substantive change to this section.

Scope. Paragraph (b) sets out the scope of the rule, and tracks the enforcement role assigned to the Commission by section 505(a)(7) of the G-L-B Act. It states that the rule applies only to information about individuals who obtain a financial product or service from a financial institution to be used for personal, family, or household purposes. The principal type of entity subject to the rule is a ''financial institution,'' a term section 509(3) of the G-L-B Act defines very broadly to mean ''any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956'' (12 U.S.C. 1843(k)). Those ''financial activities'' include not only a number of traditional financial activities specified in section 4(k) itself,[6] but also those activities that the Federal Reserve Board has found to be either closely related to banking,[7] or usual in connection with the transaction of banking or other financial operations abroad,[8] by regulation (or order or interpretation) ''in effect on the date of the enactment of the Gramm-Leach-Bliley Act.'' [9] Section 313.1(b) also lists some examples of ''financial institutions'' subject to Commission jurisdiction under the Act. Finally, this part notes that the Commission is also authorized to enforce the Act against ''other persons'' who are not financial institutions, but receive protected information from a financial institution and are subject to section 502(c) of the G-L-B Act (''Limits on Reuse of Information''), which imposes restrictions on recipients of such information as set forth in 16 CFR 313.11, *infra*.

Many industry commenters suggested revising the ''financial institution'' definition set forth in § 313.3(k) to narrow the scope to only those businesses that engage in traditional financial activities, arguing that Congress did not intend to cover businesses that conducted no such activities. On the other side, consumer commenters vigorously defended the broad scope, contending that the need to protect personal financial data extends beyond traditional financial institutions and that Congress intended to regulate a wide range of businesses that provide ''financial'' services to consumers when it enacted this statute. The G-L-B Act clearly covers more than parties in the credit, insurance, or securities industries; rather, an entity is a ''financial institution'' if it engages in any activity that the Board has determined to be a ''financial activity.''

[6] Section 4(k)(4)(A–E) states ''the following activities shall be considered to be financial in nature: (A) Lending, exchanging, transferring, investing for others, or safeguarding money or securities. (B) Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death, or providing and issuing annuities, and acting as principal, agent, or broker for purposes of the foregoing, in any State. (C) Providing financial, investment, or economic advisory services, including advising an investment company (as defined in section 3 of the Investment Company Act of 1940). (D) Issuing or selling instruments representing interests in pools of assets permissible for a bank to hold directly. (E) Underwriting, dealing in, or making a market in securities.''

[7] Section 4(k)(4)(F). The Board's list of such activities is found in 12 CFR 225.28 and 12 CFR 225.86(a). The latter subsection was added as an interim rule published by the Board in the **Federal Register** upon enactment of the G-L-B Act (65 FR 14433; Mar. 14, 2000), subject to revision after a public comment period ending on May 12, 2000. The activities listed in 12 CFR 225.28 include in certain circumstances: brokering or servicing loans; leasing real or personal property (or acting as agent, broker, or advisor in such leasing) without operating, maintaining or repairing the property; appraising real or personal property; check guaranty, collection agency, credit bureau, and real estate settlement services; providing financial or investment advisory activities including tax planning, tax preparation, and instruction on individual financial management; management consulting and counseling activities (including providing financial career counseling); courier services for banking instruments; printing and selling checks and related documents; community development or advisory activities; selling money orders, savings bonds, or traveler's checks; and providing financial data processing and transmission services, facilities (including hardware, software, documentation, or operating personnel), data bases, advice, or access to these by technological means.

[8] Section 4(k)(4)(G). The scope of the Act is not limited to activities abroad, because the text of Section 4(k)(4)(G) is ''Engaging, *in the United States*, in any Section 4(k)(4)(G) activity that (i) a bank holding company may engage in outside of the United States; and (ii) the Board has determined to be usual in connection with the transaction of banking and financial operations abroad.'' (Emphasis added.) The Board has provided a list of such activities in 12 CFR 211.5(d) and 12 CFR 225.86(b). The latter subsection was added as an interim rule published by the Board in the **Federal Register** upon enactment of the G-L-B Act (65 FR 14433; Mar. 14, 2000), subject to revision following a public comment period ending on May 12, 2000. The activities listed in 12 CFR 211.5(d) include leasing real or personal property (or acting as agent, broker, or advisor in such leasing) where the lease is functionally equivalent to an extension of credit; acting as fiduciary; providing investment, financial, or economic advisory services; and operating a travel agency in connection with financial services.

[9] Section 4(k)(4)(G) uses ''*day before the* date of'' rather than ''date of'' in the quoted phrase.

After a careful review of the comments received, the Commission finds no sound rationale for fundamentally revising the scope of the rule. Therefore, the Commission continues to interpret the act as written and has made no broad change to 16 CFR 313.1(b) in that regard.[10] However, as the Commission noted when it proposed this rule and repeats hereafter, some businesses that are technically ''financial institutions'' will have no disclosure obligations under the Act.[11] Furthermore, as is evident from the discussion of the term ''customer relationship'' that is defined in 16 CFR 313.3(i), many others will have only limited duties because they will not establish such relationships or they will be of very short duration.

Several commenters requested that the Commission clarify how its rule applies to insurance companies. The Commission notes that section 505 of G-L-B Act, which sets out the enforcement authority of the Agencies, explicitly commits the enforcement jurisdiction over ''persons engaged in providing insurance'' to state insurance authorities, thus excluding them from the Commission's authority (and, by operation of section 504(a)(1) of the G-L-B Act, from the Commission's rulemaking authority).

Several other commenters asked that the final rule state that certain transactions that are exempt from the coverage of the Truth in Lending Act (TILA; 15 U.S.C. 1601 *et seq.*) and Regulation Z (Reg. Z, 12 CFR part 226) also be treated as beyond the scope of the privacy rule. TILA and Reg. Z, which impose disclosure requirements on credit extended to consumers under certain circumstances, exempt several transactions, including those involving business, commercial, or agricultural credit. 15 U.S.C. 1603(1); 12 CFR 226.3(a). The Commission agrees that transactions that fit within the business, commercial, and agricultural exemptions from TILA and Reg. Z for these types of credit also would fall outside the scope of the privacy rule, and has amended § 313.1(b) accordingly.[12]

Several comments suggested that the rule should not apply to entities that must comply with regulations issued by the HHS that implement the HIPAA. Given the broad definition of ''financial institution'' under the G-L-B Act, certain entities are subject to these privacy rules as well as rules promulgated under HIPAA regarding appropriate handling of protected health information. Accordingly, financial institutions may be covered both by this privacy rule and by the regulations promulgated by HHS under the authority of sections 262 and 264 of HIPAA once those regulations are finalized. Based on the proposed HIPAA rules, it appears likely that there will be areas of overlap between HIPAA and financial privacy rules. For instance, under the proposed HIPAA regulations, consumers must provide affirmative authorization before a covered institution may disclose medical information in certain instances, whereas under the financial privacy rules, institutions need only provide consumers with the opportunity to opt out of disclosures. In this case, the Agencies anticipate that compliance with the affirmative authorization requirement, consistent with the procedures required under HIPAA, would satisfy the opt out requirement under the financial privacy rules. After HHS publishes its final rules, the Commission and other Agencies will consult with HHS to avoid the imposition of duplicative or inconsistent requirements.

The Commission also received several comments from colleges and universities and their representatives requesting that institutions of higher education be excluded from the definition of financial institution. The Commission disagrees with those commenters who suggested that colleges and universities are not financial institutions. Many, if not all, such institutions appear to be significantly engaged in lending funds to consumers. However, such entities are subject to the stringent privacy provisions in the Federal Educational Rights and Privacy Act (''FERPA''), 20 U.S.C. 1232g, and its implementing regulations, 34 CFR part 99, which govern the privacy of educational records, including student financial aid records. The Commission has noted in its final rule, therefore, that institutions of higher education that are complying with FERPA to protect the privacy of their student financial aid records will be deemed to be in compliance with the Commission's rule.

Section 313.2 Rule of Construction

Proposed § 313.2 of the rule sets out a rule of construction intended to clarify the effect of the examples used in the rule. As noted in the proposal, these examples are not intended to be exhaustive; rather, they are intended to provide guidance about how the rule would apply in specific situations.

Commenters generally agreed that examples are helpful in clarifying how the rule will work in specific circumstances and suggested that the Commission should include more examples. Many commenters requested that the Commission provide examples of model disclosures. Commenters also generally agreed that it is useful to state that the list of examples is not intended to be exhaustive, and that compliance with one of the examples would be deemed compliance with the regulation. A few commenters suggested that the regulation state that a financial institution is not obligated to comply with an example but has the latitude to comply with the general rule in other ways. Others stated that the examples ought to be identical in each privacy regulation adopted by the Agencies. The Commission also received comments suggesting that the Commission defer to the expertise of other agencies when considering application of its rule to entities such as credit unions or investment advisors under its jurisdiction.

The Commission believes that more examples would be helpful and has included additional examples in appropriate places throughout the rule. The Commission has also provided sample clauses in Appendix A to the rule to aid financial institutions in their drafting of privacy notices. The sample clauses are provided to illustrate the level of detail the Commission believes is appropriate. The Commission cautions financial institutions against relying on the sample clauses without determining the relevance or appropriateness of the disclosure for their operations. The Commission has used statutory terms, such as ''nonpublic personal information'' and ''nonaffiliated third parties,'' in the sample clauses to convey generally the subject of the clauses. However, a financial institution that uses these terms must provide sufficient information to enable consumers to understand what these terms mean in the context of the institution's notices. Moreover, the Commission notes that, in providing the sample disclosures, the Commission is addressing solely the

[10] However, as discussed in the definition of ''financial institution'' in § 313.3(k), the Commission has retained its interpretation that an institution is covered only if it is ''significantly engaged'' in such activities.

[11] ''Many entities that come within the broad definition of financial institution will likely not be subject to the disclosure requirements of the rule because not all financial institutions have 'consumers' or establish 'customer relationships.' '' 65 Fed. Reg. 11174, 11177 (Mar. 1, 2000).

[12] Thus, creditors may look at how this exemption is applied under Reg. Z for guidance on the scope of covered transactions under the privacy rule. It should be noted, however, that TILA exempts several other types of transactions that would be covered under the privacy rule if they are for the purpose of an individual obtaining a financial product or service as that term is defined in the privacy regulation. *See* 15 U.S.C. 1603 (2) and (3).

level of detail required and is not attempting to provide guidance on issues such as type size, margin width, ''clear and conspicuous'' generally, and so on.

The rule does not contain a statement regarding a financial institution's ability to comply with the rule in ways other than as suggested in the examples, but does provide that the examples are not exclusive. The rule also states that compliance with the examples will constitute compliance with the rule. The Commission believes that, when read together, these provisions give financial institutions sufficient flexibility to comply with the regulation but also sufficient guidance about the use of examples.

The Commission understands that the NCUA and SEC have issued, or will issue, final rules with examples that are tailored to entities under their jurisdiction. Therefore, the Commission has stated in § 313.2 that compliance by non-federally insured credit unions with credit union examples in the NCUA rule will constitute compliance with the Commission's rule. Similarly, compliance by interstate securities broker-dealers and investment advisers that are not registered with the SEC with applicable examples in the SEC rule will constitute compliance with the Commission's rule.

Section 313.3 Definitions

a. *Affiliate.* The proposal adopted the definition of ''affiliate'' that is used in section 509(6) of the G-L-B Act. An affiliation exists when one company ''controls'' (which is defined in § 313.3(g), below), is controlled by, or is under common control with another company. The definition includes both financial institutions and entities that are not financial institutions.

The Commission received comparatively few comments in response to this definition. A few commenters requested that the final rule state that a credit union service organization will be deemed to be an affiliate of every credit union that has an interest in it. The Commission has declined to adopt this suggestion. If the relationship between a credit union and a credit union service organization satisfies the test for affiliation set out in the statute and regulation, then an affiliation exists.

In light of the comparatively few comments received and the nature of those comments, the Commission adopts the definition of ''affiliate'' as proposed.

b. *Clear and conspicuous.* Under the proposed rule, various notices must be ''clear and conspicuous.'' The proposed rule defines this term to mean that the notice must be reasonably understandable and designed to call attention to the nature and significance of the information contained in the notice. The proposal did not mandate the use of any particular technique for making the notices clear and conspicuous, but provided examples of how a notice may be made clear and conspicuous. As noted in the preamble to the proposed rule, each financial institution retains the flexibility to decide for itself how best to comply with this requirement.

The Commission received a large number of comments on this proposed definition. Some commenters favored adopting the definition as proposed, with some of these advocating that the final rule add a requirement that disclosures must be on a separate piece of paper in order to ensure that they will be conspicuous. Others stated that the definition was unnecessary, given the experience financial institutions have in complying with requirements that disclosures mandated by other laws be clear and conspicuous. Several commenters made the related point that the rule proposed is inconsistent with requirements in other consumer protection regulations such as Reg. Z and the Truth in Savings regulation (Regulation DD, 12 CFR part 230), which require only that a disclosure be reasonably understandable. Many of these commenters expressed concern that the examples would invite litigation because of ambiguities inherent in terms used in the examples in the proposed rule such as ''ample line spacing,'' ''wide margins,'' and ''explanations * * * subject to different interpretations.'' A few commenters questioned how the requirement would work in a document that contains several disclosures that each must be clearly and conspicuously disclosed, while others raised questions about how a disclosure may be clear and conspicuous on a web site. These comments are addressed below.

New standard for ''clear and conspicuous'' The Commission recognizes that the proposed definition articulates the concept of ''clear and conspicuous'' in ways perhaps not familiar to some commenters. However, the Commission included the phrase ''designed to call attention to the nature and significance of the information contained'' to provide added meaning to the term ''conspicuous.'' The Commission believes that this standard, when coupled with the existing standard requiring that a disclosure be readily understandable, likely will result in notices to consumers that communicate effectively the information needed by consumers to make an informed choice about the privacy of their information, including whether to transact business with a financial institution.

The standard for clear and conspicuous adopted by the Commission in this rulemaking applies solely to disclosures required under the privacy rules. Disclosures governed by other rules requiring clear and conspicuous disclosures (such as Reg. Z) are beyond the scope of this rulemaking.

Examples of ''clear and conspicuous'' The Commission recognizes that many of the examples require judgment in their application. The Commission believes, however, that more prescriptive examples, while perhaps easier to conform to, likely would result in requirements that would be inappropriate in a given circumstance. To avoid this result, the examples provide generally applicable guidance about ways in which a financial institution may make a disclosure clear and conspicuous. The Commission notes that the examples of how to make a disclosure clear and conspicuous are not mandatory. A financial institution must decide for itself how best to comply with the general rule and may use techniques not listed in the examples. To address these concerns, the Commission has incorporated several of the commenters' suggestions for ways to make the guidance more helpful.

Combination of several ''clear and conspicuous'' notices. A document may combine several disclosures that each must be clear and conspicuous. The final rule provides an example, in § 313.3(b)(2)(ii)(E), of how a financial institution may make disclosures conspicuous, including disclosures on a combined notice. In order to avoid the potential conflicts envisioned by several commenters between two different requirements, the final rule does not mandate precise specifications for how various disclosures must be presented.

Because the Commission believes that privacy disclosures may be clear and conspicuous when contained in a document containing other disclosures, the rule does not mandate that disclosures be provided on a separate piece of paper. Such a requirement is not necessary and would significantly increase the burden on financial institutions. Moreover, it would not necessarily provide the most effective notice in all circumstances.

Disclosures on web pages. Several commenters requested guidance on how they may clearly and conspicuously

disclose privacy-related information on their Internet sites. The Commission recognizes that disclosures over the Internet present some issues that will not arise in paper-based disclosures. There may be web pages within a financial institution's website that consumers may view in a different order each time they access the site, aided by hypertext links. Depending on the customer hardware and software used to access the Internet, some web pages may require consumers to scroll down to view the entire page. To address these issues, the Commission has included a statement in the example in § 313.3(b)(2)(iii) concerning Internet disclosures informing financial institutions that they may comply with the rule if they use text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice. In addition, a financial institution is to place either a notice or a conspicuous link on a page frequently accessed by consumers, such as a page on which transactions are conducted.

Given current technology, there are a range of approaches a financial institution could take to comply with the rule. For example, a financial institution could use a dialog box that pops up to provide the disclosure before a consumer provides information to the institution. Another approach would be a simple, clearly labeled graphic located near the top of the page or in close proximity to the financial institution's logo, directing the customer, through a hypertext link or hotlink, to the privacy disclosures on a separate web page.

For the reasons advanced above, the Commission has adopted the definition of ''clear and conspicuous,'' with the changes previously described and with certain other changes intended to make the definition easier to apply.

c. *Collect.* The statute requires a financial institution to include in its initial and annual notices a disclosure of the categories of nonpublic personal information that the institution collects. The proposal defined ''collect'' to mean obtaining any information that is organized or retrievable on a personally identifiable basis, irrespective of the source of the underlying information. This definition was included to provide guidance about the information that a financial institution must include in its notices and to clarify that the obligations arise regardless of whether the financial institution obtains the information from a consumer or from some other source.

Commenters suggested that the final rule treat information that is not organized and retrievable in an automated fashion as not ''collected.'' This approach would exclude separate documents not included in a file. The Commission disagrees that information should not be deemed to be collected simply because it is not retrievable in an automated fashion. The Commission believes that the method of retrieval is irrelevant to whether information should be protected under the rule. The Commission agrees, however, that the scope of the regulation should be refined, and has changed the definition of ''collect'' by using language taken from the Privacy Act of 1974 (5 U.S.C. 552a).

Other commenters requested that the rule clarify that information that is received by a financial institution but then immediately passed along without otherwise disclosing, using, or maintaining a copy of the information is not ''collected'' as this term is used in the final rule. The Commission believes that merely receiving information without maintaining it would not be ''collecting'' the information. The final rule reflects this by stating that the information must be organized or retrievable by the financial institution. Otherwise, the definition of ''collect'' is adopted as proposed.

d. *Company.* The proposal defined ''company,'' which is used in the definition of ''affiliate,'' as any corporation, limited liability company, business trust, general or limited partnership, association, or similar organization.

The Commission received no substantive comments on this proposed definition.[13] Accordingly, the Commission adopts the definition of ''company'' as proposed.

e. *Consumer.* The G-L-B Act distinguishes ''consumers'' from ''customers'' for purposes of the notice requirements imposed by the Act. A financial institution is required to give a ''consumer'' the notices required under Title V only if the institution intends to disclose nonpublic personal information about the consumer to a nonaffiliated third party for purposes other than as permitted by section 502(e) of the statute (as implemented by §§ 313.14 and 313.15). By contrast, a financial institution must give all ''customers'' a notice of the institution's privacy policy at the time of establishing a customer relationship and annually thereafter during the continuation of the customer relationship.

The proposed rule defined ''consumer'' to mean an individual (and his or her legal representative) who obtains, from a financial institution, financial products or services that are to be used primarily for personal, family, or household purposes. Because ''financial product or service'' is defined to include the evaluation by a financial institution of an application to obtain a financial product or service (*see* further discussion of this point, below), a person becomes a consumer even if the application is denied or withdrawn. An individual also would be deemed to be a consumer (as well as a customer) of a financial institution that purchases the individual's account from some other institution.

The Commission received a large number of comments on this proposed definition, raising questions about how the definition would apply in a variety of situations. These comments are addressed below.

Distinction between ''consumer'' and ''customer.'' While many agreed with the distinction drawn in the proposal between ''consumer'' and ''customer,'' a few commenters suggested that no distinction between ''consumer'' and ''customer'' should be made, given that, in these commenters'' views, the statute appears to use the terms interchangeably. The Commission believes, however, that the distinction was deliberate and that the rule should implement it accordingly. A plain reading of the statute supports the conclusion that Congress created one set of protections for anyone who obtains a financial product or service (*i.e.,* who receives a financial institution's privacy policy and opt out notice only if a financial institution intends to disclose nonpublic personal information to nonaffiliated third parties), and an additional set of protections for anyone who establishes a relationship of a more lasting nature than an isolated transaction with a financial institution (*i.e.,* who gets a notice of the institution's privacy policy at the time of establishing a customer relationship, and annual notices as appropriate thereafter). Because the statute tailors the notice requirements to the type of relationship an individual has with a financial institution, that distinction is preserved in the rule.

Applicants as consumers. Many of the comments received by the Commission concerning the proposed definition of ''consumer'' disagreed that someone should be deemed a consumer of a financial institution simply by

[13] However, the Commission did receive a few comments asking that sole proprietors be excluded from the definitions of both ''company'' and ''financial institution.'' Those comments are discussed in the context of § 313.3(k).

virtue of the institution evaluating an application. These commenters maintained that the individual has not obtained a financial product or service, as is required by the statutory definition of ''consumer.'' The Commission believes that the better reading of the G-L-B Act is that an individual has obtained a financial product or service when a financial institution evaluates information provided to the financial institution for the purpose of the individual obtaining some other financial product or service. Financial institutions frequently provide a range of services in connection with the delivery of a financial product. Included within these will be the evaluation by the financial institution of information provided by an individual. In certain instances, such as when an individual is shopping for the best rate on a mortgage loan or the lowest premium for an insurance policy, that evaluation may be the sole financial product or service obtained. In other instances, the evaluation may be one of several services provided that lead up to the eventual establishment of a customer relationship. In either case, the individual will have obtained a financial product or service from the financial institution when the financial institution evaluates the information and informs the individual of the outcome of that evaluation.

In addition to being consistent with the language of the statute, the proposed definition of ''consumer'' is consistent with one of the primary purposes of Title V of G-L-B Act, namely, to enable an individual to limit the sharing of nonpublic personal information by a financial institution with a nonaffiliated third party. The information provided by a person to a financial institution before a customer relationship is established is likely to contain precisely the types of information that the statute is designed to protect. This information is no less deserving of protection simply because an application is denied or withdrawn. For these reasons, the Commission has retained the individual whose application is evaluated by a financial institution as an example of ''consumer'' in § 313.3(e)(2)(i).

Loan sales. Several commenters requested clarification of whether an individual becomes a consumer in various other scenarios involving loans. Commenters posited a wide variety of examples, which, if each were to be addressed specifically in the rule, would require a final rule of enormous complexity and detail. The Commission believes that a rule setting forth a general principle that is flexible enough to be applied in the array of loan transactions posited by the commenters is more appropriate. Towards this end, the Commission's rule provides, by example at § 313.3(e)(2)(iv), that a person will be a consumer of any entity that holds ownership or servicing rights to an individual's loan.[14] Financial institutions that own or service a loan are providing a financial product or service to the individual borrower in question. In some cases, the product or service is the funding of the loan, directly or indirectly. In other cases, the product or service is the processing of payments, sending account-related notices, responding to consumer questions and complaints about the handling of the account, and so on. The rule defines ''consumer'' in a way that covers individuals receiving financial products or services in each of these situations.

Agents of financial institutions. Several commenters agreed with the principle set out in the proposed rule that an individual should not be considered to be a consumer of an entity that is acting as agent for a financial institution. These commenters noted that the financial institution that hires the agent is responsible for that agent's conduct in carrying out the agency responsibili ties. The Commission agrees that the purposes of the G-L-B Act will be met provided the activities of the agent are the responsibility of the financial institution, and, therefore, the financial institution fulfills any obligations regarding the agent's handling of consumer information that otherwise would fall on the agents.[15] Of course, those providing services to a financial institution will also be subject to the limitations on reuse of information. *See* § 313.3(e)(2)(v).

Legal representative. The Commission also agrees with the suggestion made by several commenters that the definition of ''consumer'' should clarify that the obligations stemming from a consumer relationship may be satisfied by dealing either with the individual who obtains a financial product or service from a financial institution *or* that individual's representative. The Commission does not intend for the rule to require a financial institution to send opt out and initial notices to *both* the individual and the individual's legal representatives and has amended the final rule accordingly in § 313.3(e)(1).

Trusts. The Commission and the other Agencies received several comments concerning whether an individual who obtains financial services in connection with trusts is a consumer or customer of a financial institution. Several commenters urged the Agencies to exempt generally a financial institution from the requirements of the rule when it acts as a fiduciary, or, in the alternative, to clarify the categories of individuals that are considered to be customers. Commenters proposed, for example, that individuals who are beneficiaries with current interests should be identified as customers, whereas individuals who are only contingent beneficiaries should not be customers. Other commenters stated that when the financial institution serves as trustee of a trust, neither the grantor nor beneficiary is a consumer or customer under the rule. In these commenters' view, the trust itself is the institution's ''customer,'' and, therefore, the rule should not apply to a financial institution when it acts as trustee. These commenters also stated that when a financial institution is a trustee, it serves as a fiduciary and is subject to other obligations to protect the confidentiality of the beneficiaries' information that are more stringent than those under the provisions in the G-L-B Act. Similarly, these and other commenters claimed that an individual who is a participant in an employee benefit plan administered or advised by a financial institution does not qualify as a consumer or customer. The commenters opined that the plan sponsor, or the plan itself, is the ''customer'' for the purposes of the proposed rule. These commenters contended that plan participants have no direct relationship with the financial institution and, in any event, the financial institution is authorized to use information that would be covered under the G-L-B Act only in accordance with the directions of the plan sponsor. The commenters concluded, therefore, that the regulations should specifically exclude individuals who are participants in an employee benefit plan from the definition of consumer.

The definition of ''consumer'' in the G-L-B Act does not squarely resolve whether the beneficiary of a trust is a consumer of the financial institution that is the trustee. One consideration is that a financial institution that is a trustee assumes obligations as a fiduciary, including the duty to protect

[14] Such a person may not be a customer, however. *See* explanation of how the definition of ''customer'' will be applied in the loan context, in the discussion of the definition of § 313.3(h) and (i) below. *See also* § 313.4(c)(2) and (3)(ii) for further discussion concerning when a borrower establishes a customer relationship in the context of a loan sale.

[15] Of course, in some cases two institutions will each provide a financial service to the consumer as part of the same transaction, such as a loan broker that locates a creditor who makes a loan to the individual, in which case the consumer will have a customer relationship with both financial institutions.

the confidentiality of the beneficiaries' information, that are consistent with the purposes of the G-L-B Act and enforceable under state law. The Commission agrees with the commenters who concluded that, when the financial institution serves as trustee of a trust, neither the grantor nor the beneficiary is a consumer or customer under the rule. Instead, the trust itself is the institution's ''customer,'' and therefore, the rule does not apply because the trust is not an individual. Similarly, the Commission has excluded an individual who is a beneficiary of a trust or a plan participant of an employee benefit plan from the definitions of ''consumer'' and ''customer.'' Nevertheless, the Commission believes that an individual who selects a financial institution to be a custodian of securities or assets, for example in an IRA, is obtaining a financial product or service from the financial institution and is, therefore, a ''consumer'' under the G-L-B Act. The Commission has included examples in the rule that appropriately illustrate this interpretation of the G-L-B Act in §§ 313.3(e)(2)(vi)–(viii) and 313.3(i)(2)(i)(D).

Requirements arising from consumer relationship. While the proposed and final rule defines ''consumer'' broadly, this will not result in any additional burden to a financial institution in situations where (a) no customer relationship is established and (b) the institution does not intend to disclose nonpublic personal information about a consumer to nonaffiliated third parties. Under the final rule, a financial institution is under no obligation to provide a consumer who is not a customer with any privacy disclosures unless it intends to disclose the consumer's nonpublic personal information to nonaffiliated third parties outside the exceptions in §§ 313.14 and 313.15. A financial institution that wants to disclose a consumer's nonpublic personal information to nonaffiliated third parties is not prohibited by the rule from doing so, if the requisite notices are delivered and the consumer does not opt out. Thus, a financial institution that does not wish to be subject to the disclosure obligations of the rule as it applies to consumers who are not customers may simply decide not to share consumers' information with nonaffiliated third parties. Conversely, if a financial institution determines that the benefits of such sharing outweigh the attendant burdens, the financial institution is free to do so provided it notifies consumers about the disclosure and affords them a reasonable opportunity to opt out. In this way, the rule attempts to strike a balance between protecting an individual's nonpublic personal information and minimizing the burden on a financial institution.

f. *Consumer reporting agency.* The proposal adopted the definition of ''consumer reporting agency'' that is used in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f)). It is used in §§ 313.6(c), 313.12(a), and 313.15(a)(5) of the final rule.

The Commission received no comments suggesting any changes to this definition. Accordingly, the definition is adopted as proposed.

g. *Control.* The proposal defined ''control'' using the tests applied in section 23A of the Federal Reserve Act (12 U.S.C. 371c). This definition is used to determine when companies are affiliated (see discussion of § 313.3(a), above), and would result in financial institutions being considered as affiliates regardless of whether the control is by a company or individual.

The Commission received few comments in response to this definition. Some commenters suggested that a definition that did not require 25% ownership be adopted, while others suggested adopting a test focused solely on percent of stock owned in a company so as to avoid the uncertainties arising from a ''control in fact'' test.

The Commission believes that the proposed test is sufficiently well established and has concluded that an alternative test to be used solely in the privacy rule could create confusion. The Commission also believes that any test based only on stock ownership is unlikely to be flexible enough to address all situations in which companies are appropriately deemed to be affiliated and that including the stock ownership as one measurement of control provides necessary flexibility. Accordingly, the Commission adopts the definition of ''control'' as proposed.

h. *Customer.* The proposal defined ''customer'' as any consumer who has a ''customer relationship'' with a particular financial institution. As is explained more fully in the discussion of § 313.4, below, a consumer is a customer of a financial institution when the consumer has a continuing relationship with the institution.

The Commission received a large number of comments on the definition of ''customer'' and ''customer relationship.'' Given the interdependence of the two terms, the following analysis of the comments received will address both under the heading ''customer relationship.''

i. *Customer relationship.* The proposed rule defined ''customer relationship'' as a continuing relationship between a consumer and a financial institution whereby the institution provides a financial product or service that is to be used by the consumer primarily for personal, family, or household purposes. As noted in the proposal, a one-time transaction may be sufficient to establish a customer relationship, depending on the nature of the transaction. A consumer would not become a customer simply by repeatedly engaging in isolated transactions that by themselves would be insufficient to establish a customer relationship, such as withdrawing funds at regular intervals from an ATM owned by an institution at which the consumer has no account. However, an individual who becomes the client of a loan brokerage, tax preparation firm, or financial counseling service would be a customer. The proposal also stated that a consumer would have a customer relationship with a financial institution that makes a loan to the consumer and then sells the loan but retains the servicing rights. The Commission received a large number of comments on this definition, as discussed below.

Point at which one becomes a customer. The Commission received many comments in response to the definitions of ''customer'' and ''customer relationship.'' Some commenters criticized what they considered to be the ill-defined line distinguishing consumers from customers. These commenters stated that the proposed distinction makes it difficult for a financial institution to know when the obligations attendant to a customer relationship arise. Several suggested that the distinction should be based on when a consumer and financial institution enter into a written contract for a financial product or service.

The Commission recognizes that the distinction between consumers and customers will, in some instances, require a financial institution to evaluate whether the particular facts of its consumer transactions fit within the definition of customer relationship. In those cases where an individual engages in a transaction that is isolated in nature (such as ATM transactions, purchases of money orders, or cashing of checks), the individual will not have established a customer relationship as a result of that transaction. In other situations, where a consumer typically would receive some measure of service such that the consumer's contact with the financial institution is more significant (such as would be the case when a consumer

borrows money, obtains investment advice, or becomes the client of an institution for the purpose of receiving tax preparation, loan brokerage, or credit counseling services), a customer relationship will be established. In those cases, the nature of the relationship indicates that it is not an isolated transaction, even though it may be short-term in duration.[16] The Commission believes that the distinction set out in the proposed rule, as further clarified by the examples in the final rule regarding the establishment of a customer relationship, provides sufficiently clear principles that can be applied to most fact situations that arise in the financial marketplace.

Customer relationship defined by written contract. The Commission agrees with those commenters who consider the execution of a written contract by a consumer and financial institution as clear evidence that a customer relationship has been established. The proposal cited the execution of a written contract as an example of when a customer relationship is established, and the final rule retains that example in § 313.4(c)(3)(i)(B). However, a test based solely on whether there is a written contract could inappropriately exclude situations in which an individual is a customer of a financial institution as a result of obtaining, for instance, financial, economic, or investment advisory services from a financial institution. Accordingly, the final rule does not define a customer relationship solely by the execution of a written contract.

Purchase of insurance. Other commenters suggested that, in the context of financial institutions that engage in the sale of insurance, the customer should be the policyholder and not the beneficiary. The Commission agrees and has retained the example in § 313.3(i)(2)(i)(C) of purchasing an insurance product as one situation in which a customer relationship is formed.[17] In this case, the person obtaining a financial product or service from the financial institution is the person purchasing the policy. The beneficiaries would be recipients of the insurance proceeds, thereby entitling them to the protections afforded consumers.

Sales of loans. As previously noted, several commenters raised questions in the context of loan sales. Many commenters stated that, under the final rule, a person should not be considered a customer of two financial institutions when the originating bank sells the servicing rights. A point consistently made by these commenters was that a borrower would be equally well protected with less risk of confusion if the borrower is deemed to be a customer of only one entity in connection with a loan, with that entity perhaps being the party with whom the borrower communicates about the loan. The Commission believes that it is appropriate to consider a loan transaction as giving rise to only one customer relationship, with the recognition that this customer relationship may be transferred in connection with a sale of part or all of the loan. In this way, the borrower will not be inundated by privacy notices (but rather will normally receive annual notices from the loan servicer), many of which might be from subservicers that the borrower did not know had any connection to his or her loan. However, that customer will remain a consumer of the entity that transfers the servicing rights, as well as a consumer of any other entity that holds an interest in the loan.

In order to satisfy the statutory requirement that a customer receive an annual notice from a financial institution until that relationship terminates, the final rule provides that the borrower must be deemed to have a customer relationship with at least one of the entities that hold an interest in the loan. A financial institution that makes a loan, retains it in its portfolio, and provides servicing for the loan clearly would have a customer relationship with the borrower. More complex, however, are situations in which servicing is sold or investors purchase a partial interest in a loan. The Commission has adopted an approach designed to ensure that a customer receives annual notices for the duration of the customer relationship from the most appropriate financial institution.

Under the final rule, as stated in § 313.3(i)(2)(i)(B), a customer relationship will be established as a general rule with the financial institution that makes a loan to an individual. This customer relationship then will attach to the entity providing servicing. Thus, if the originating lender retains the servicing, it will continue to have a customer relationship with the borrower and will be obligated to provide annual notices for the duration of the customer relationship. If the servicing is sold, then the purchaser of the servicing rights will establish a customer relationship (and the originating lender will have a consumer relationship with the borrower). *See* § 313.3(i)(2)(ii)(B). In this way, the borrower will be entitled to receive an initial notice and annual notices from the loan servicer, but will not be inundated by initial and annual notices from entities that hold interests in the loan but are unknown to the consumer (and who do not share the consumer's nonpublic personal information with unaffiliated third parties).

Collection agencies that purchase accounts in their own name. The Commission received a substantial number of comments from different types of debt collectors and their representatives. This section addresses several comments the Commission received concerning the proposed rule's differentiation between collectors who assist creditors in collecting delinquent accounts, and those who purchase them in their own name.[18] The Commission also received comments from all types of collection agencies on other points. Several contested the Commission's treatment of debt collectors as financial institutions.[19] Others were concerned that the rule would prohibit communications with a creditor that retained ownership on the account and hired the agency to obtain payment from debtors.[20]

Representatives of two major trade associations of debt collectors pointed to the definitions set forth in section 803 of the Fair Debt Collection Practices Act, which specifically exempts any ''creditor'' collecting its own accounts in its own name from being within the definition of a ''debt collector'' subject to that statute, and the case law holding that the ''creditor'' exemption does not include debt collectors that purchase defaulted accounts in their own name

[16] Many of the customer relationships established by institutions under the Commission's jurisdiction may well be short-term, as can be seen from the examples in § 313.5(b)(2) of when a customer relationship terminates.

[17] Despite its lack of enforcement jurisdiction over persons providing insurance, the Commission retains this example because it may be useful in evaluating analogous situations. Some commenters also asked for further clarification of ''purchase'' in this context. The Commission does not believe such clarification is necessary and has retained the example as proposed.

[18] ''A consumer has a ''customer relationship'' with a debt collector that purchases an account from the original creditor (because he or she would have a credit account with the collector), but not with a debt collector that simply attempts to collect amounts owed to the creditor.'' 65 FR 11174 at 11176 (Mar. 1, 2000).

[19] Those issues are discussed under §§ 313.1(b), 313.3(k) and 313.4.

[20] This fear is unfounded, because such a communication by a collection agency reporting to a creditor that has retained ownership of an account would be permitted under § 313.15(a)(2)(iv). That section allows communications to parties holding a legal interest relating to the consumer, which would certainly include a creditor that owns the debt.

for collection.[21] The commenters argued that, because the FDCPA does not treat collection agencies that purchase defaulted accounts in their own name as creditors, the G-L-B Act should not be interpreted to do so. In addition, debt buyers stated that they frequently made bulk purchases of defaulted accounts from creditors, immediately discarded and never even attempted to collect many of the accounts they purchased, and were unable to locate many of the account debtors from whom they wanted to collect amounts due.

The Commission recognizes that these businesses have some attributes of creditors who buy active accounts (where the debtors clearly become customers of the account purchaser) and some attributes of regular debt collectors who attempt to collect amounts due on behalf of the creditor (where the debtors clearly remain the creditor's customer). After careful consideration of the comments and the purposes of the Act, the Commission retains its view that if a business purchases a defaulted account for collection, it may establish a ''customer relationship'' with the account debtor. However, such a relationship occurs only in those instances where the agency locates the individual and tries to obtain payments on the debt. This approach reflects the reality that the collector has purchased the account (albeit for less than it would pay for a current account) and avoids the result that otherwise the individual would not have a ''customer relationship'' with anyone because the former relationship with the creditor will have been terminated. At the same time, it responds to industry commenters that contested the Commission's previous position that purchase of the account automatically establishes a customer relationship. The applicable example in § 313.3(i)(2)(i)(J) makes it clear that a debt buyer does not have a customer relationship if it does not attempt to collect payments from, or is unable to locate, the individual named on an account it has purchased.

Brokers. Several commenters suggested that the use of a mortgage broker, or other business that procures credit on behalf of a consumer, such as financing to purchase an automobile, should not create a customer relationship. The Commission disagrees. A relationship between such a business and a consumer is more than an isolated transaction, given that the broker will likely provide significant services for a consumer, such as providing information or advice about financing options, actively assisting the consumer in contacting potential financing sources, analyzing financial information, or performing credit checks. In some cases, the broker will also negotiate with other financial institutions on the consumer's behalf and/or assist with paperwork and loan closings. In light of the nature of the services provided by a loan broker or other credit arranger in assisting the consumer with financial transactions, it is appropriate to consider the business to be a financial institution that establishes a customer relationship when it undertakes to arrange or broker a home mortgage loan or other credit for the consumer. The final rule reflects this conclusion in § 313.3(i)(2)(i)(E).

IRA Custodians. The final rule adds an example in § 313.3(i)(2)(i)(D) to clarify that an individual will be deemed to establish a customer relationship when a financial institution acts as a custodian for securities or assets in an IRA. This example is consistent with the explanation set out above in the discussion of ''consumer'' concerning trusts.

j. *Federal functional regulator.* The proposal sought comment on a definition of ''government regulator'' that included all of the Agencies and State insurance authorities under the circumstances identified in the definition.[22]

The few comments that were received on this definition suggested that it be expanded to include additional governmental entities. The Commission notes that, for purposes of the privacy rule, this term (which does not include the Commission) is relevant only in the discussion of when a financial institution may disclose information to a law enforcement agency. The exception as stated in the statute uses the term ''federal functional regulator'' (*see* section 502(e)(5)), which term is defined in the statute at section 509(2) and also includes the Commission and Secretary of the Treasury, for purposes of the exception permitting disclosures to law enforcement agencies. The Commission has decided simply to use the statutory term.

k. *Financial institution.* The Commission's proposed rule defined financial institution as ''any institution the business of which is engaging in activities that are financial in nature as described in section 4(k) of the Bank Holding Company Act * * *'' Through the examples, the Commission expressed its view that an institution is a financial institution ''the business of which is engaging in activities that are financial in nature'' only if the entity is significantly engaged in such activities. The Commission received numerous comments concerning this definition.

Some commenters requested that the Commission adopt the definition of financial institution contained in the other Agencies' definition. The other Agencies defined financial institution as ''any institution the business of which is engaging in activities that are financial in nature *or incidental to such financial activities* as described in section 4(k) of the Bank Holding Company Act.'' Section 509(3) of the G–L–B Act defines the term as ''any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956.'' Section 4(k) of the Bank Holding Company Act refers to three types of activities that the Board may determine permissible for financial holding companies: those that are financial in nature, those that are incidental to such financial activity, and those that are complementary to financial activities. The Commission interprets the G-L-B Act to refer to those activities in Section 4(k) that are described as financial in nature at present, and not to include automatically those activities that the Board later determines are incidental or complementary to financial activities. Such activities are not necessarily themselves financial activities and, therefore, should not have an impact on the definition of financial institution. Thus, the final rule incorporates the statutory language in § 313.3(k).[23]

Given the breadth of the definition, some commenters requested that the Commission provide a definitive list of the entities that are subject to the rule. The Commission deems it inappropriate to publish such a definitive list. The institutions covered by the rule currently are defined by reference to the comprehensive list of activities found at section 4(k)(4) of the Bank Holding Company Act.[24] The Commission has

[21] 15 U.S.C. 1692a(4) and 1692a(6). *Cirkot v. Diversified Fin. Sys., Inc.,* 839 F. Supp. 941, 944–45 (D. Conn. 1993); *Holmes v. Telecredit Service Corp.,* 736 F. Supp. 1289, 1293 (D. Del. 1990); *Kimber v. Federal Fin. Corp.,* 668 F. Supp. 1480, 1485–86 (D. Ala. 1987).

[22] This term was used in the exception set out in § 313.11(a)(4) of the proposal as it related to disclosures to law enforcement agencies, ''including government regulators.''

[23] *See also* the discussion of the effective date at § 313.18, *infra.* Section 4(k) of the Bank Holding Company Act established procedures whereby the Board can add activities to the list of activities that it is permissible for financial holding companies to engage in. To the extent these later added activities are financial activities, and not incidental activities, the rule will not be effective as to those new financial institutions until the Commission so determines.

[24] See footnotes 5–8 and accompanying text, *supra.* These are activities either specified in

reformatted and added additional examples of financial institutions in the final rule to guide the analysis of whether a particular entity is a financial institution through reference to section 4(k)(4) and particular sections of the Board regulations that are incorporated therein by reference.

The Commission received several comments on the ''significantly engaged'' standard set forth in the examples in the proposed rule. A few expressed concern that the ''significantly engaged'' test was too imprecise to allow some businesses to know whether they were within the definition, usually suggesting alternatives that would exclude the industries they represent. The final rule does not define ''significantly engaged.'' The revenue tests suggested by some commenters are too inflexible to take into consideration all instances where an institution may be significantly engaged in a financial activity. The final rule retains the flexibility of the ''significantly engaged'' standard and provides guidance through examples. To that end, the Commission has moved the ''significantly engaged'' language into the text of the final rule and retains in the final rule those examples from the proposed rule of entities that are and are not significantly engaged in a financial activity. A retail business that issues its own credit card directly to consumers is a financial institution significantly engaged in the extension of credit, but a retail business that merely allows its retail clients to make payments through occasional lay-away plans is not significantly engaged in a financial activity. Similarly, a small merchant that informally extends credit when it ''runs a tab'' for some individuals is not significantly engaged in the business of extending credit. The Commission believes that the concept of ''significantly engaged'' is sufficiently clear to provide guidance to most entities in analyzing their specific factual situations.

Many commenters, especially some representatives of the consumer debt collection industry,[25] expressed concern at the breadth of the definition and asserted that Congress could not have intended to include all institutions that engage in the activities referenced in Section 4(k). The plain language of the statute, however, dictates that breadth and grants the Commission no authority to exclude particular entities from the definition. The broad scope of the Act, and the comments received by the Commission, are also discussed above in more detail in the context of § 313.1(b). While it is not possible to discuss every potential financial institution in detail, the Commission specifically sought comment on certain of the activities listed in section 4(k) and the Board regulations that are incorporated by reference.

The proposed rule acknowledged that one of the activities characterized as financial in nature in Section 4(k)(4) of the Bank Holding Company Act is operating a travel agency in connection with offering financial services.[26] The Commission received few comments on the extent to which travel agents operate in connection with financial services. The comments did indicate that travel agents generally do sell travelers checks, trip insurance, and travel insurance, all of which constitute financial products or services. However, the Commission does not consider a travel agency's operations to be ''in connection with offering financial services'' and therefore covered simply because it offers travelers checks or travel related insurance to their travel clients. Rather, the Commission interprets the G-L-B Act to cover travel agencies only if their travel-related services are offered in addition to offering other financial services.[27] This would cover, for example, entities that offer credit, investment, or insurance products or services, and also offer travel-related services to their clients. For these types of entities, travel operations would thereby become covered services and their travel transactions would be protected by the G-L-B Act.[28]

Some commenters requested clarification concerning whether certain Internet industries are affected by the rule. The comments in this regard did not provide sufficient detail for the Commission to evaluate all of the concerns of the commenters, but the Commission notes that institutions operating on-line, like those operating off-line, will have to evaluate (1) whether they are engaged in a financial activity, and (2) if so, whether they have consumers or customers that trigger the disclosure or other requirements of the Act. On a related issue, the Commission notes that one of the financial activities incorporated by reference into Section 4(k) of the Bank Holding Company Act is:

> ''providing data processing and data transmission services, facilities (including data processing and data transmission hardware, software, documentation, or operating personnel), data bases, advice, and access to such services, facilities, or data bases by any technological means, if * * * [t]he data to be processed or furnished are financial, banking, or economic * * *.''

12 CFR 225.28 (b)(14). The Commission notes with respect to this activity that financial software and hardware manufacturers, as described, are financial institutions but will have no disclosure obligations if they sell only to businesses. Furthermore, in the case of an isolated one-time sale of software or hardware to a consumer, their disclosure obligations would be very limited. In addition, this language brings into the definition of financial institution an Internet company that compiles, or aggregates, an individual's on-line accounts (such as credit cards, mortgages, and loans) at that company's web site as a service to the individual, who then may access all of its account information through that Internet site.

Many entities that come within the broad definition of financial institution will likely not be subject to the disclosure requirements of the rule because not all financial institutions have ''consumers'' or establish ''customer relationships.'' Several commenters supported this distinction and the Commission retains it here. For example, management consulting is a ''financial activity'' but it is not likely

---

Section 4(k)(4) itself, or are activities listed in Board regulations referenced in Section 4(k)(4) already in effect on the effective date of the G–L–B Act. This list of activities may expand as the Board exercises its authority to add additional activities that are financial in nature pursuant to Section 4(k)(1–3) of the Bank Holding Company Act.

[25] The statute is clear that debt collection agencies are financial institutions under its terms. As noted in the discussion of the definition of ''financial institution'' below, the statute treats a broad range of activities as ''financial in nature.'' Section 509(3) of the G-L-B Act defines the term to mean ''any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956.'' Section 4(k)(4)(F) of the Bank Holding Company Act includes all financial activities deemed by the Federal Reserve Board ''to be so closely related to banking or managing or controlling banks as to be a proper incident thereto.'' In Regulation Y, 12 CFR 225.28(b)(2)(iv), the Board specifically designated ''collection agency services'' as such a financial activity.

[26] *See* footnote 5 of the Commission's discussion of the proposal at 65 FR 11176. Section 4(k)(4)(G) of the Bank Holding Company Act includes all financial activities conducted in the United States deemed by the Federal Reserve Board ''to be usual in connection with the transaction of banking or other financial operations abroad.'' In Regulation K, 12 CFR 211.(d)(15), the Board specifically designated ''[o]perating a travel agency * * * in connection with financial services'' as such a financial activity.

[27] This analysis is consistent with an interim rule published by the Board at 12 CFR 225.86(b)(2), in which it characterized the travel agency activity ''operating a travel agency in connection with financial services offered by the financial holding company or others.'' 65 FR 14433, 14439 (Mar. 17, 2000).

[28] *See* the Commission's discussion of ''financial product or service'' in the next section, as it relates to the Act's inapplicability to nonfinancial products or services of financial institutions.

that any individual obtains management consulting services for personal, family or household purposes. Likewise, courier services, data processors, and real estate appraisers who perform services for a financial institution, but do not provide financial products or services to individuals, will not be required to make the disclosures mandated by the rule because they do not have ''consumers'' or ''customers'' as defined by the rule.[29] The Commission declines to adopt a definitive list, as requested by some commenters, of all of the financial institutions that do not have consumers and customers. Such a list inevitably will not be exclusive and may include some institutions that operate so that in some instances they have consumers and customers and in others they do not.

Some commenters suggested that sole proprietors be exempt from the definition, but provided no helpful rationale for doing so, while others requested clarification as to whether nonprofit entities could be financial institutions covered by the rule. Whether or not a commercial enterprise is operated by a single individual is not determinative in analyzing whether the entity is a ''financial institution.'' If an individual is in the ''business of * * * engaging in financial activities * * *,'' that ''business'' is included within the ''financial institution'' definition.[30] Similarly, nothing in the definition of financial institution excludes nonprofit entities from the definition of financial institution.

Few commenters addressed proposed § 313.3(j)(3)(iii), which incorporated the Act's exemption for institutions chartered by Congress to engage in secondary market sales and similar transactions related to consumers, as long as the institution does not sell or transfer nonpublic personal information to a nonaffiliated third party. This exemption applies even if the chartered institution sells or transfers information as permitted by the exceptions to the notice and opt out requirements in proposed §§ 313.10 and 313.11 (§§ 313.14 and 313.15 in the final rule). The Commission also sought comment on whether it should require chartered institutions, as a condition of their exemption, to enter into a confidentiality agreement with any nonaffiliated third parties with whom they share information pursuant to the exceptions. Chartered institutions supported the interpretation; one commenter contended that such additional language was not in keeping with the intent of the exemption. The Commission believes that its interpretation merely operates to allow chartered institutions to continue their normal business, and does not permit them (or any party receiving information from them) to disclose information unrestrained. In accord with the limitations on reuse and redisclosure in section 502(c) of the G–L–B Act, both chartered institutions and recipients of nonpublic personal information are limited in that regard. The Commission has adopted the provision as proposed.

l. *Financial product or service.* The proposal defined ''financial product or service'' as a product or service that a financial institution could offer by engaging in an activity that is financial in nature under section 4(k) of the Bank Holding Company Act of 1956. The proposal's definition included the financial institution's evaluation of information collected in connection with an application by a consumer for a financial product or service even if the application ultimately is rejected or withdrawn. It also included the brokerage and distribution of information about a consumer for the purpose of assisting the consumer in obtaining a financial product or service.

The most frequent comment on this proposed definition was that the evaluation of application information should not be considered a financial product or service. For the reasons advanced above in the discussion of the definition of ''consumer,'' the Commission concludes that it is appropriate to retain evaluation activity within the scope of financial product or service covered by the rule. Evaluation is one of many financial services provided by financial institutions. Moreover, a consumer is likely to provide the type of information that the statute is designed to protect in the course of obtaining the financial institution's evaluation.

An entity's status as a financial institution does not cause every product or service offered by that entity to be a financial product or service. A retailer that issues its own credit card directly to consumers provides a financial service (credit) to consumers who utilize the card; but when that same retailer sells merchandise, it provides a nonfinancial product or service (retail sale of merchandise).

The Commission has retained the essence of the proposed definition, but has revised § 313.(l)(1) to mirror its change to the definition of ''financial institution'' in § 313.3(k) and eliminated the word ''distribution'' from § 313.3(l)(2) because it is not intended to mean anything different from ''brokerage'' and, therefore, its use invites confusion.

m. *Nonaffiliated third party.* The proposal defined ''nonaffiliated third party'' as any person (which includes natural persons as well as corporate entities) except (1) an affiliate of a financial institution and (2) a joint employee of a financial institution and a third party. The proposal clarified the circumstances under which a company that is controlled by a financial institution pursuant to that institution's merchant banking activities or insurance company activities would be a ''nonaffiliated third party'' of that financial institution.

The Commission received very few comments in response to this proposed definition. One commenter requested that the final rule provide that a disclosure of information to someone who is serving as a joint employee of two financial institutions should be deemed to have been disclosed to both financial institutions. The Commission disagrees with this result. Instead, the Commission believes it is appropriate to deem the information to have been given to the financial institution that is providing the financial product or service in question. Thus, if an employee of a mortgage lender is a dual employee with a securities firm, information received by that person in connection with a securities transaction conducted with the securities firm would be deemed to have been received by the securities firm.

The Commission notes that its proposal omitted a section included in the other Agencies' rules relating to companies engaged in merchant banking, investment banking, or investment activities described in section 4(k)(4)(H–I) of the Bank Holding Company Act. For purposes of consistency with the rules to be adopted by the other Agencies, the Commission has included it at § 313.3(m)(2). Otherwise, the final rule defines ''nonaffiliated third party'' as proposed.

n. *Nonpublic personal information.* Section 509(4) of the G-L-B Act defines ''nonpublic personal information'' to mean ''personally identifiable financial information'' that is provided by a consumer to a financial institution, results from any transaction with the

[29] If such financial institutions receive consumers' nonpublic personal information from nonaffiliated financial institutions pursuant to one of the exceptions set forth in §§ 313.14 and 313.15, however, they would be required to observe the § 313.11 limitations on reuse and redisclosure of that information.

[30] An individual who provides a financial service only informally (*e.g.,* preparing tax forms without remuneration for friends or family, or as community service) is not likely significantly engaged in a financial activity.

consumer or any service performed for the consumer, or is otherwise obtained by the financial institution. It also includes any ''list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information.'' The statute excludes publicly available information (unless provided as part of the list, description or other grouping described above), as well as a list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using nonpublic personal information. The statute does not define either ''personally identifiable financial information'' or ''publicly available information.''

The proposed rule restated the categories of information described above and presented two alternative approaches to identifying what information would be regarded as publicly available (and therefore, as a general rule, outside the definition of ''nonpublic personal information''). Alternative A deemed information as publicly available only if a financial institution *actually obtained* the information from a public source while Alternative B treated information as publicly available if a financial institution *could* obtain it from such a source. Both Alternatives A and B included within the definition of ''nonpublic personal information'' publicly available information that is provided as part of a list, description, or other grouping of consumers. In addition to requesting comment on Alternatives A and B, the Commission requested comment concerning whether a variation of the two alternatives should be adopted that would require a financial institution to undertake reasonable procedures to establish that information is, in fact, publicly available.

Commenters favoring Alternative A noted that it provided the greatest protection for consumers by treating anything the consumer gives to a financial institution to obtain a financial product or service as nonpublic personal information. Under Alternative A, this protection would be lost only if a financial institution actually obtained the information from a public source. These commenters also preferred the bright-line distinction drawn by treating as nonpublic personal information any information given by a consumer to obtain a financial product or service or information that results from transactions between a financial institution and a consumer. However, the majority of those commenting on this issue favored Alternative B, noting that this alternative was consistent with the statute and would be far less burdensome on financial institutions. These commenters suggested that a requirement that the information actually be obtained from a public source would impose needless burdens on financial institutions (by requiring, for instance, that a financial institution ''tag'' information they obtained from public records) and is not required by the statute.

The final rule incorporates the benefits of both alternatives. Under the final rule, information will be deemed to be ''publicly available'' and therefore excluded from the definition of ''nonpublic personal information'' if a financial institution has a reasonable basis to believe that the information is lawfully made available to the general public from one of the three categories of sources listed in the rule. *See* § 313.3(p)(1). The final rule provides that a financial institution will have a ''reasonable basis'' for believing that information is lawfully made available if the financial institution has taken steps to determine whether the information is of the type that is available to the general public, whether an individual can direct that the information not be made available to the general public, and, if so, that the financial institution's particular consumer has not so directed. In this way, a financial institution will be able to avoid the burden of having to actually obtain information from a public source, but will not be free simply to assume that information is publicly available without some reasonable basis for that belief.

An example of information a financial institution might have a reasonable basis to believe is publicly available, cited in the final rule, is the fact that someone has a loan that is secured by a mortgage, as long as the financial institution has determined that the mortgage information is included on the public record in the relevant jurisdiction. *See* § 313.3(p)(3)(iii)(1). The rule also explains that a financial institution will have a reasonable basis to believe that a telephone number is publicly available only if the institution has either located the number in a telephone book or has been informed by the consumer that the number is not an unlisted telephone number. *See* § 313.3(p)(3)(iii)(2). This approach is based on the underlying principle that a financial institution should not automatically assume that an individual's information is publicly available, especially if a consumer has some measure of control over the public availability of the information.

With regard to some types of information that may be available to the general public, the extent to which a consumer can control the release of that information should be well known. For example, in most jurisdictions, a borrower has no choice about whether a lender will make a mortgage a matter of public record; a lender must do so in order to protect its security interest. In the case of a telephone number, it is well established that a person may request that his or her number be unlisted; thus, the financial institution will have to takes steps to determine whether a particular consumer has exercised that option. In other instances, there will be more variation on the general availability of the information and the consumer's right to direct that it not be disclosed. Some jurisdictions, for example, make driver's license information more available than others.[31] In evaluating whether it is reasonable to believe that information is publicly available, a financial institution must consider whether the information is of a type that a consumer could keep from being a matter of public record.

To implement the Act's complex definition of ''nonpublic personal information'' that is provided in the statute, the final rule adopts a definition that consists, generally speaking, of (1) personally identifiable financial information, plus (2) a consumer list (and publicly available information pertaining to the consumers on that list) that is derived using personally identifiable financial information that is *not* publicly available. From that body of information, the final rule excludes publicly available information (except as noted above) and any consumer list that is derived without using personally identifiable financial information that is not publicly available. *See* § 313.3(n)(1) and (2). Examples are provided in § 313.3(n)(3) to illustrate how this definition applies in the context of consumer lists.

o. *Personally identifiable financial information.* The proposed rule defined ''personally identifiable financial information'' to include information that a consumer provides to a financial institution in order to obtain a financial product or service, information resulting from any transaction between the consumer and the financial institution involving a financial product or service,

[31] The Driver's Privacy Protection Act, 18 U.S.C. 2721–2725, restricts the states' ability to disclose a driver's personal information without the driver's consent. *Reno* v. *Condon* __ U.S. __, 120 S. Ct. 666 (2000).

and information about a consumer a financial institution otherwise obtains in connection with providing a financial product or service to the consumer. The proposed rule also treated the fact that someone is a customer of a financial institution as personally identifiable financial information. In essence, the proposed rule treated any personally identifiable information as financial if it was obtained by a financial institution in connection with providing a financial product or service to a consumer. The Commission noted in the preamble to the proposed rule that this interpretation may result in certain information being covered by the rule that may not be considered intrinsically financial, such as health status.

The Commission received a large number of comments in response to this definition, most of which stated that the definition inappropriately included certain identifying information that is not financial, such as name, address, and telephone number. Many others maintained that ''personally identifiable financial information'' should not include the fact that someone is a customer of a financial institution. These commenters typically noted that many customer relationships are matters of public record (such as would be the case, for instance, anytime a transaction results in the recordation of a security interest) while other customer relationships are matters of public knowledge (because consumers frequently disclose the relationships by writing checks, using credit cards, and so on). Many commenters stated that aggregate data about a financial institution's customers that lack personal identifiers should not be considered personally identifiable financial information.

Treatment of identifying information as financial. The Commission continues to believe that any information should be considered financial information if it is requested by a financial institution for the purpose of providing a financial product or service. This approach is consistent with the broad definition of ''financial institution'' used in the statute, which encompasses not only traditional financial activities (such as banks, mortgage lenders, finance companies), but also a large number of entities that engage in activities not traditionally considered financial (such as financial career counselors, insurance companies, and data processors). As a consequence of that definition, the range of information that has a bearing on the terms and availability of a financial product or service or that is used by a financial institution in connection with providing a financial product or service is extremely broad and may include, for instance, medical information and other sorts of information that might not be thought of as financial.

Many commenters, including several hundred private investigators, expressed concern about the need for ready access to identifying information to locate people attempting to evade their financial obligations. These commenters consistently suggested that names, addresses, and telephone numbers should not be treated as financial information. However, financial institutions rely on a broad range of information that they obtain about consumers, including information such as addresses and telephone numbers, when providing financial products or services. Location information is used by financial institutions to provide a wide variety of financial services, from the sending of checking account statements to the disbursing of funds to a consumer. Other information, such as the maiden name of a consumer's mother often will be used by a financial institution to verify the consumer's identity. The Commission concluded that it would be inappropriate to carve out certain items of information that a particular financial institution might rely on when providing a particular financial product or service.

The Commission notes that names, addresses, and telephone numbers, if publicly available, will not be subject to the opt out provisions of the statute unless that information is ''derivative information'' (*i.e.,* information that is part of a list, description, or other grouping of consumers that is derived from personally identifiable financial information that is not publicly available). Thus, in instances involving specific requests about individuals, a financial institution still may disclose information about the individual that the institution has a reasonable basis to believe is publicly available, provided that in so doing the institution does not disclose the existence of a customer relationship (unless the relationship is a matter of public record, as in the case of most mortgage loans). Moreover, in instances when a consumer does not opt out, a financial institution may disclose any nonpublic personal information to a nonaffiliated third party provided that the disclosure is consistent with the institution's opt out and privacy notices.

Customer relationship as ''personally identifiable financial information.'' The Commission disagrees with those commenters who maintain that customer relationships should not be considered to be personally identifiable financial information. Information that a particular person has a customer relationship identifies that person, and thus is personally identifiable. This information also is financial, because it communicates that the person in question has a transaction involving a financial product or service with a financial institution. While this information could in certain cases be a matter of public record, that does not change the analysis of whether the information is personally identifiable financial information.

Changes made to the definition. The final rule makes various stylistic changes to the definition to make it easier to read and understand. In addition, the final rule adds to the examples of information covered by the rule any information that the institution collects through a ''cookie.'' [32] *See* § 313.3(o)(2)(F). This illustrates one of the various means by which a financial institution may ''otherwise obtain'' information about a consumer in connection with providing a financial product or service to that consumer.

An example in § 313.3(o)(2)(ii)(B) clarifies that aggregate information or blind data lacking personal identifiers is not covered by the definition of ''personally identifiable financial information.'' The Commission agrees with those commenters who opined that such data, by definition, do not identify any individual.

p. *Publicly available information.* The proposal defined ''publicly available information'' to include information that is lawfully made available to the public from official public records (such as real estate recordations or security interest filings), information from widely distributed media (such as a telephone book, television or radio program, or newspaper), and information that is required to be disclosed to the general public by Federal, State, or local law (such as securities disclosure documents). The proposed rule stated that publicly available information from widely distributed media would include information from an Internet site that is available to the general public without requiring a password or similar restriction.

As noted in the discussion of ''nonpublic personal information,'' the Commission proposed two versions of the definition of ''publicly available information.'' The final rule more closely tracks the statute while

[32] A cookie is a small text file placed on a consumer's computer hard drive by a web server. The cookie transmits information back to the server that placed it.

incorporating the benefits of both alternatives.

Several commenters questioned the appropriateness of excluding information from the definition of ''publicly available information'' if a person who seeks to obtain the information over the Internet must have a password or comply with a similar restriction. These commenters made the point that many Internet sites are available to a large number of people, each of whom need a user name and identification number to access the sites. Several of these commenters suggested that it is more appropriate to focus on whether the information was lawfully placed on the Internet.

The Commission agrees and has amended the final rule to remove the reference to passwords or similar restrictions from the example of the Internet as a ''widely distributed'' medium of communication. In its place, the Commission has substituted a standard requiring that the information be available on an unrestricted basis, and has then specified that a site is not restricted merely because an Internet service provider or a site operator requires a fee or password as long as access is otherwise available to the general public. The traditional use of passwords is to confine the access of individual customers to specific, individual information. However, website operators, in particular, may require user identifications and passwords as a method of tracking access rather than restricting access to the information available through the website. Fees may be levied to enhance the revenue of the Internet service provider or site operator rather than restrict access. Therefore, the Commission believes that the definition of ''widely distributed media'' should properly focus on whether the information is lawfully available to the general public, rather than on the type of medium from which information is obtained.

The concept of information being lawfully obtained was included in the proposal, and is retained in the final rule. Thus, information unlawfully obtained will not be deemed to be publicly available notwithstanding that it may be available to the general public through widely distributed media.

The following example illustrates how ''nonpublic personal information,'' ''personally identifiable financial information,'' and ''publicly available information'' will work under the final rule. Assume that Mary provides a mortgage lender with information in order to obtain a loan to finance a home purchase, and the same information to a retail store to open a credit card account. Under the final rule, all of this information would be personally identifiable financial information. Once Mary establishes the customer relationships she seeks, the fact that Mary is a mortgage loan customer and a credit card customer at the financial institutions also would be personally identifiable financial information.

Certain information provided by Mary, such as her name and address, may be publicly available. If the mortgage lender has a reasonable basis to believe that this information is publicly available, and if the information was included on a list of all of the institution's mortgage loan customers, then her name and address would fall outside the definition of ''nonpublic personal information'' in those jurisdictions where mortgages are a matter of public record. However, Mary's name and address would be protected as nonpublic personal information if the retailer wanted to include those items on a list of holders of its proprietary credit card. The difference in treatment stems from the distinction drawn in the statute between lists prepared using publicly available information (as would be the case in the mortgage loan hypothetical) and lists prepared using information that is not publicly available (as would be the case in the credit card hypothetical).

The Commission concludes that this relatively complex approach is mandated by the statute's definition of ''nonpublic personal information.'' The final rule also is consistent with the fact that certain relationships are matters of public record, and, therefore, less deserving of protection from disclosure.

q. *You.* The Commission used the pronoun ''you'' to refer to financial institutions within its jurisdiction in the proposal and defined ''you'' to mean those entities.

The Commission received no comments in response to this definition and adopts the definition set forth in the proposed rule.

Section 313.4 Initial Privacy Notice to Consumers Required

The G-L-B Act requires a financial institution to provide an initial notice of its privacy policies and practices in two circumstances. For customers, the notice must be provided at the time of establishing a customer relationship. For consumers who are not customers, the notice must be provided prior to disclosing nonpublic personal information about the consumer to a nonaffiliated third party.

The proposed rule implemented these requirements by mandating that a financial institution provide the initial notice to an individual prior to the time a customer relationship is established and the opt out notice prior to disclosing nonpublic personal information to nonaffiliated third parties. These notices were required to be clear and conspicuous and to accurately reflect the institution's privacy policies and practices. The proposal also set out standards governing when a customer relationship is established and how a financial institution is to provide notice.

The Commission received many comments on proposed § 313.4. Most of the comments raised questions about the time by which initial notices must be provided, whether new notices are required for each new financial product or service obtained by a customer, the point at which a customer relationship is established, and how initial notices may be provided.

Providing initial notices ''prior to'' time customer relationship is established. Many commenters stated that, because the statute requires only that the initial notice be provided ''at the time of establishing a customer relationship,'' the regulation should not require that the notice be provided ''prior to'' the point at which a customer relationship is established. These commenters were concerned that the rule could be interpreted as requiring a financial institution to provide disclosures at a point different from when they must provide other federally mandated consumer disclosures during the process of establishing a customer relationship.

In response to these comments, the Commission has clarified the timing for providing initial notices. The final rule provides that, as a general rule, the initial notice must be given not later than the time when a financial institution establishes a customer relationship. *See* § 313.4(a)(1). As in the proposal, the initial notices may be provided at the same time a financial institution is required to give other notices, such as those required by the Board's regulations implementing the TILA. This approach, like the approach taken in the proposed rule, strikes a balance between (1) ensuring that consumers will receive privacy notices at a meaningful point along the continuum of ''establishing a customer relationship'' and (2) minimizing unnecessary burdens on financial institutions that may otherwise result if the final rule were to require financial institutions to provide consumers with a series of notices at different times in a transaction.

Providing notices after customer relationship is established. Several commenters stated that the rule should provide financial institutions with the flexibility to deliver the initial notice after the customer relationship is established under certain circumstances. These commenters posited several situations in which a customer relationship is established without face-to-face contact between the consumer and financial institution. For example, collection agencies that purchase accounts in default noted that it frequently takes time to locate debtors on such accounts (and that sometimes they do not even try to do so.) The commenters stated that delivery of the initial notice *before* the customer relationship is established in these situations would be impractical, and a requirement along those lines would have a significant adverse effect on the ability to provide a financial product or service to a consumer as quickly as the consumer desires.

The Commission believes that it is appropriate for financial institutions to have flexibility in certain circumstances to provide the initial notice at a point after the customer relationship is established. To accommodate the wider range of situations presented by the commenters, the Commission has modified the relevant examples so that they now are more broadly applicable. As stated in the final rule in § 313.4(e), a financial institution may provide the initial notice within a reasonable time after establishing a customer relationship in two instances. First, notice may be provided after the fact if the establishment of the customer relationship is not at the customer's election. *See* § 313.4(e)(1)(i). This might occur, for instance, when a credit account is sold. Second, a notice may be sent after establishing a customer relationship when to do otherwise would substantially delay the consumer's transaction and the consumer agrees to receive the notice at a later time. *See* § 313.4(e)(1)(ii). An example of this would be when a transaction is conducted over the telephone and the customer desires prompt delivery of the item purchased. Another example of when this might occur is when a lender (other than a college or university) establishes a customer relationship with an individual under a student loan program as described in the final rule where loan proceeds are disbursed promptly without prior communication between the bank and the customer.

In most situations, and particularly where the establishment of a customer relationship is in person, a financial institution should give the initial notice at a point when the consumer still has a meaningful choice about whether to enter into the customer relationship. The exceptions listed in the examples, while not exhaustive, illustrate the less frequent situations when delivery either would pose a significant impediment to the conduct of a routine business practice or the consumer agrees to receive the notice later in order to obtain a financial product or service immediately.

In circumstances when it is appropriate to deliver an initial notice after the customer relationship is established, a financial institution should deliver the notice within a reasonable time thereafter. For example, a debt buyer that has purchased a defaulted account for collection in its own name would be authorized by § 313.4(e)(2)(i) to provide its privacy notice shortly after locating the debtor. Several commenters requested that the final rule specify precisely how many days a financial institution has in which to deliver the notice under these circumstances. However, the Commission believes that a rule prescribing the maximum number of days would be inappropriate because (a) the circumstances of when an after-the-fact notice is appropriate are likely to vary significantly, and (b) a rule that attempts to accommodate every circumstance is likely to provide more time than is appropriate in many instances. Thus, rather than establish an inflexible rule, the Commission has elected to retain the more general rule as set out in the proposal in § 313.4(e)(1).

Nothing in the rule is intended to discourage a financial institution from providing an individual with a privacy notice at an earlier point in the relationship if the institution wishes to do so in order to make it easier for the individual to compare its privacy policies and practices with those of other institutions in advance of conducting transactions.

New notices not required for each new financial product or service. Several commenters asked whether a new initial notice is required every time a customer obtains a financial product or service from that financial institution. These commenters suggested that the public would not materially benefit from repeated disclosures of the same information, and that requiring additional initial notices to be provided to the same consumer would be burdensome on financial institutions.

The Commission agrees that it would be burdensome, with little corresponding benefit to the public, to require a financial institution to provide the same consumer with additional copies of its initial notice every time the consumer obtains a financial product or service. Accordingly, the final rule states, in § 313.4(d)(2), that a financial institution will satisfy the notice requirements when an existing customer obtains a new financial product or service if the institution's initial, revised, or annual notice (as appropriate) is accurate with respect to the new financial product or service.

Joint accountholders. The majority of comments on how to provide notice suggested that the final rule state that a financial institution is not obligated to provide more than one notice to joint accountholders. Several of these commenters noted that disclosure obligations arising from joint accounts are well settled under other rules, such as the regulations implementing the Equal Credit Opportunity Act (Regulation B, 12 CFR part 202,) and TILA. Under both Reg. B and Reg. Z, a financial institution is permitted to give only one notice. The authorities cited include requirements that the financial institution give disclosures, as appropriate, to the ''primary applicant'' if this is readily apparent (in the case of Reg. B; *see* 12 CFR 202.9(f)) or to a person ''primarily liable on the account'' (in the case of Reg. Z; *see* 12 CFR 226.5(b)).

The Commission agrees that a financial institution should be allowed to provide initial notices in a manner consistent with other disclosure obligations. There are also circumstances, however, where more than one of the joint account holders may want separate notices. Therefore, the final rule states in § 313.9 that the financial institution may send one notice, but must honor requests from one or more account holders for separate notices. Even absent a request, a financial institution may, in its discretion, provide notices to each party to the account. This situation might arise, for instance, when a financial institution does not want one opt out election to apply automatically to all joint accountholders (*see* discussion of how to provide opt out notices, below).

Mergers. A few commenters requested guidance on what notices are required in the event of a merger of two financial institutions or an acquisition of one financial institution by another. In such a situation, the need to provide new initial (and opt out) notices to the customers of the entity that ceases to exist will depend on whether the notices previously given to those customers accurately reflect the policies and practices of the surviving entity. If

they do, the surviving entity will not be required under the rule to provide new notices.

As was stated in the preamble to the proposed rule, a financial institution must maintain any protections that it represents it will provide in its privacy notices. Financial institutions must take appropriate measures to adhere to their stated policies and practices.

Section 313.5 Annual Privacy Notice to Customers Required

Section 503 of the G-L-B Act requires a financial institution to provide notices of its privacy policies and practices at least annually to its customers ''during the continuation'' of a customer relationship. The proposed rule implemented this requirement by requiring a clear and conspicuous notice that accurately reflects the privacy policies and practices then in effect to be provided at least once during any period of twelve consecutive months. The proposed rule noted that provisions governing how to provide an initial notice also would apply to annual notices, and stated that a financial institution would not be required to provide annual notices to a customer with whom it no longer has a continuing relationship.

Several commenters requested that the final rule permit annual notices to be given each calendar year, instead of every twelve months. A variation suggested by a few commenters was to state that notices must be provided during each calendar year, with no more than 15 months elapsing between mailings. To clarify the extent of financial institutions' flexibility, the final rule retains the general rule requiring annual notices but then provides an example, in § 313.5(a)(2), stating that a financial institution may select a calendar year as the 12-month period within which notices will be provided and provide the first annual notice at any point in the calendar year following the year in which the customer relationship was established. The final rule also requires that a financial institution apply the 12-month cycle to its consumers on a consistent basis.

Several commenters suggested that a financial institution be permitted to make the annual notice available upon request only, particularly if there have been no material changes to the notice since it was last delivered or the customer has opted out. These commenters maintained that little value is added by providing customers with additional copies each year of the same information. Some suggested that financial institutions be permitted to provide a ''short-form'' annual notice, in which the institution informs its customers that there has been no change to its privacy policies and practices and that the customers may obtain a copy upon request.

The Commission has not amended the final rule to permit this approach, for two reasons. First, the Commission interprets the statute as contemplating complete disclosures annually to all customers during the duration of the customer relationship. Section 503 of the G-L-B Act states that ''not less than annually during the continuation of [a customer] relationship, a financial institution shall provide a clear and conspicuous disclosure to such consumer [*i.e.,* one with whom a customer relationship has been formed], . . . of such financial institution's policies and practices with respect to'' the information enumerated in the statute. The Commission believes that this provision contemplates a full set of disclosures to each customer once a year.

Second, the clarifications made in the final rule to the disclosure provisions make it clear that a financial institution is not required to provide a lengthy and detailed privacy notice to comply with the rule. Small institutions that do not share information with third parties beyond the statutory exceptions should be able to provide a short, streamlined notice. The rule also permits a financial institution to provide annual notices to customers over the institution's web site if the customer conducts transactions electronically and agrees to such disclosures (*see* additional discussion of this flexibility, below, in § 313.9). As a result, the final rule achieves much of the burden reduction sought by those requesting a short-form annual notice option.

Most of the remaining comments received in response to proposed § 313.5 addressed the sections governing when a customer relationship is terminated. Some noted that the examples used ''consumer'' when ''customer'' was appropriate, and the final rule is revised accordingly. A few commenters, including retailers and some whose business related to real estate transactions, stated that the example of no communication with a customer for twelve months should be amended to clarify that promotional materials would not be considered a communication about the relationship sufficient to reactivate a dormant or terminated customer relationship. These commenters generally suggested that the rule be tied to communications initiated by the customer. The Commission agrees that a communication that merely informs a person about, or seeks to encourage use of, a financial institution's products or services is not the type of communication that signifies an ongoing relationship. The final rule has been amended in § 313.5(b)(2)(vii) to reflect that the distribution of promotional materials will not prolong a customer relationship under the rule. The Commission disagrees, however, that the test should focus on whether there has been any customer-initiated contact, because there will be instances in which the customer will not initiate a contact with a financial institution within the relevant time period but nonetheless has an ongoing relationship.

Section 313.6 Information To Be Included in Initial and Annual Privacy Notices

Section 503 of the G-L-B Act identifies the items of information that must be included in a financial institution's initial and annual notices. Section 503(a) of the G-L-B Act sets out the general requirement that a financial institution must provide customers with a notice describing the institution's policies and practices with respect to, among other things, disclosing nonpublic personal information to affiliates and nonaffiliated third parties. Section 503(b) of the Act identifies certain elements that must be addressed in that notice.

The proposed rule implemented section 503 by requiring a financial institution to provide information concerning:

- The categories of nonpublic personal information that a financial institution may collect;
- The categories of nonpublic personal information that a financial institution may disclose;
- The categories of affiliates and nonaffiliated third parties to whom a financial institution discloses nonpublic personal information, other than those to whom information is disclosed pursuant to an exception in section 502(e) of the G-L-B Act;
- The financial institution's policies with respect to sharing information about former customers;
- The categories of information that are disclosed pursuant to agreements with third party service providers and joint marketers and the categories of third parties providing the services;
- A consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties;
- Any disclosures regarding affiliate information sharing opt outs a financial

institution is providing under the FCRA; and

• The financial institution's policies and practices with respect to protecting the confidentiality, security, and integrity of nonpublic personal information.

The Commission received a large number of comments concerning these requirements, with the majority of comments making the points summarized below.

Level of detail required. Many commenters offered the general observation that the level of detail that would be required under the proposed rule would result in lengthy, complicated, and ultimately confusing disclosures. These comments have led the Commission to clarify the level of detail that is required in a financial institution's initial and annual disclosures to contain.

Neither the Act nor this rule requires a financial institution to publish lengthy disclosures that identify with precision every type of information collected or disclosed, the name of every entity with whom the financial institution shares information, a complete description of the technical specifications of methods used by the institution to protect its customers' records, or the identity of each employee who has access to the records. Instead, the Commission has concluded that the statute, by focusing on ''categories'' of information and recipients of information, is intended to require notices that provide consumers with a general description of the third parties to whom a financial institution discloses nonpublic personal information, the types of information it discloses, and the other information about the institution's privacy policies and practices listed above. The Commission's intent is that the notice must be reasonably designed to be meaningful to consumers. The final rule, like the proposal, permits a financial institution to comply with these notice requirements by providing a description that accurately represents its privacy policies and practices. The Commission believes that in most cases the initial and annual disclosure requirements can be satisfied by disclosures contained in a tri-fold brochure.

To address commenters' concerns about the likelihood that consumers will not read long, detailed disclosures, the Commission has revised the examples of the disclosures set out in proposed § 313.6(e), which appears in the final rule at § 313.6(c), to clarify the level of detail that it thinks is appropriate under the G-L-B Act. Sample clauses have been provided in Appendix A to the rule, and guidance for certain institutions has been set out below in Section D. Because the examples are not exclusive, the final rule permits a financial institution to use categories different from those provided in the examples, thereby providing additional flexibility for financial institutions in complying with the disclosure requirements. In addition, the language in § 313.6(a) that precedes the items of information to be addressed in the initial notice has been amended to clarify that a financial institution is required only to address those items that apply to the institution. Thus, for instance, if a financial institution does not disclose nonpublic personal information to third parties, it may simply omit any reference to the categories of affiliates and nonaffiliated third parties to whom the institution discloses nonpublic personal information. The Commission has made these changes to clarify financial institutions' obligations under the statute and thereby eliminate unnecessary confusion.

The required content is the same for both the initial and annual notices of privacy policies and practices. While the information contained in the notices must be accurate as of the time the notices are provided, a financial institution may prepare its notices based on current and anticipated policies and practices.

The Commission received conflicting suggestions relating to disclosures required about information provided to service providers and joint marketers. Some industry commenters suggested that the example in § 313.6(a)(5) required the same specificity as other disclosures and that it should be collapsed into § 313.6(a)(1–4). Some consumer advocates asked for more detail with respect to these disclosures, because consumers cannot opt out of them. The Commission believes that the example in § 313.6(a)(5) appropriately requires a ''separate statement'' on this point, and that this is sufficient to alert consumers about this practice. Therefore, it retains the example as proposed.

Short-form initial notice. The Commission has reconsidered the need to give consumers a copy of a financial institution's complete initial notice when there is no customer relationship. In these circumstances, the Commission believes that the objectives of the statute can be accomplished in a less burdensome way than was proposed and has exercised its exemptive authority as provided in section 504(b) to create an exception to the general rule that otherwise requires a financial institution to provide both the initial and opt out notices to a consumer before disclosing nonpublic personal information about that consumer to nonaffiliated third parties.

This exception is set out in § 313.6(d) of the final rule, which states that a financial institution may provide a ''short-form'' initial privacy policy notice along with the opt out notice to a consumer with whom the institution does not have a customer relationship. The short-form notice, along with the opt out notice, must clearly and conspicuously state that the disclosure containing information about the institution's privacy policies and practices is available upon request and provide one or more reasonable means by which the consumer may obtain a copy of the notice. This approach reflects the conclusion that consumers who do not become customers of a financial institution generally will have less interest in the privacy policies of that financial institution and will benefit from obtaining a concise, but meaningful, opt out notice that informs the consumer about the categories of their information the institution intends to disclose and the categories of nonaffiliated third parties that will receive the information. Consumers who are interested in the more complete privacy disclosures will be provided with a convenient means to obtain them.

Information about affiliate sharing. Another point made by several commenters in response to proposed § 313.6 was that the rule should not include a requirement that categories of affiliates with whom a financial institution shares information be included in the initial and annual notices. These commenters pointed out that the statute specifically requires disclosures of categories of nonaffiliated third parties only, and that the only statutorily mandated disclosures concerning affiliate sharing are disclosures required, if any, concerning affiliate sharing pursuant to section 603(d)(2)(A)(iii) of the FCRA.[33] These commenters concluded that the Commission, by expanding the disclosure requirements in the manner

[33] Section 603(d)(2)(A)(iii) excludes from the definition of ''consumer report'' the communication of certain consumer information among affiliated entities if the consumer is notified about the disclosure of such information and given an opportunity to opt out of the disclosure of that information. The information that can be disclosed to affiliates under this provision includes information from consumer reports. It also includes personal information provided directly by consumers to institutions in applications for financial products or services, such as information on income and assets.

prescribed in the proposed rule, would be exceeding its rulemaking authority and imposing unnecessary burdens on financial institutions.

The language and legislative history of section 503 support requiring disclosures of affiliate sharing beyond what may be required by the FCRA. First, section 503(b) does not state that the items listed therein are to be the only items set out in a financial institution's initial and annual disclosures. Instead, it uses the nonrestrictive phrase ''shall include'' when discussing the contents of the disclosures, thereby preserving flexibility for the Commission (which was expressly granted authority under section 503(a) to prescribe rules governing these notices) to require that additional items be addressed in the disclosures consistent with those specifically enumerated.

Second, section 503(a) provides that the financial institution shall provide in its initial and annual notices ''a clear and conspicuous disclosure * * * of such financial institution's policies and practices with respect to—(1) disclosing nonpublic personal information to affiliates and nonaffiliated third parties, consistent with section 502, including the categories of information that may be disclosed; * * *.'' While the FCRA disclosures would be a subset of the disclosures required by section 503(a)(1), they may not be sufficient to fully satisfy that requirement.

Third, the legislative history of the G-L-B Act suggests that Congress intended for the disclosures to provide more information about affiliate sharing than what may be required under the FCRA.[34] That history underscores the Congressional intent of ensuring that individuals are given the opportunity to make informed decisions by reviewing the privacy policies and practices of financial institutions. The Commission believes that limiting the disclosures about affiliate sharing just to those disclosures required under the FCRA would frustrate that purpose.

Disclosures of the FCRA opt out right. Another frequent comment was that a financial institution should not be required to include FCRA disclosures in its annual notices. As previously discussed, section 503(b)(4) of the G-L-B Act requires a financial institution's initial and annual notice to include the disclosures required, if any, under section 603(d)(2)(A)(iii) of the FCRA. The proposed rule implemented section 503(b)(4) of the G-L-B Act by including the requirement that a financial institution's initial and annual notice include any disclosures a financial institution makes under section 603(d)(2)(A)(iii) of the FCRA. Several commenters pointed out that the FCRA requires disclosures of a consumer's right to opt out of affiliate sharing only once. They noted that the G-L-B Act states, in section 506(c), that nothing in the G-L-B Act is to be construed to modify, limit, or supersede the operation of the FCRA. The ''if any'' language of section 503(b)(4), read in the context of section 506, suggests that, since at most only one notice must be provided under the FCRA, section 503 should require only one FCRA disclosure under the privacy rule. The commenters concluded that, by requiring more notices than are required under the FCRA, the Commission would be violating this express preservation of the FCRA.

In order to comply with the requirement of the G-L-B Act that it disclose its policies and practices with respect to sharing information with affiliated and nonaffiliated third parties, a financial institution, must describe the circumstances under which it will be sharing information with affiliates. Clearly, the ability of consumers to opt out of affiliate information sharing under the FCRA affects a financial institution's policies and practices with respect to disclosing information to its affiliates. The Commission finds that failing to include this information and an explanation of how the opt out right may be exercised would make the disclosures incomplete. Thus, a financial institution must include this information in its initial and annual notices.

The commenters' reading of sections 503 and 506 is wrong. Section 503 does not distinguish between the disclosures to be provided in the initial notice from those to be provided in the annual notice. Thus, a plain reading of section 503 suggests that any disclosures that are required under the FCRA must be included in both the initial and annual notices.

The ''if any'' language is a recognition that not all institutions provide FCRA notices because not all institutions engage in the type of affiliate sharing covered by the FCRA. By requiring the FCRA notice to appear as part of the annual notice under the privacy rule, the Commission is not modifying, limiting, or superseding the operation of the FCRA; financial institutions will have exactly the same FCRA obligations following the effective date of the privacy rule as they had before. The only difference will be that, as is required by the G-L-B Act, a financial institution's initial and annual disclosures about its privacy policy and practices will need to reflect how the financial institution complies with the affiliate sharing provisions of the FCRA.

Disclosures of the right to opt out. Other commenters suggested that the final rule eliminate the requirement that the initial and annual notices contain disclosures about a consumer's right to opt out. These commenters pointed out that the statute does not specifically require these disclosures.

As previously discussed, section 503(a) of the statute requires a financial institution to disclose its policies and practices with respect to sharing information, both with affiliated and nonaffiliated third parties. Given that a financial institution's practices with respect to sharing nonpublic personal information with nonaffiliated third parties will be affected by the opt out rights created by the statute, an institution will need to describe these opt out rights in order to provide a complete disclosure that satisfies the statute.

Other comments. Many commenters expressed support for a number of the provisions in proposed § 313.6. For instance, several commenters noted their agreement with the approach of permitting a financial institution to state generally that it makes disclosures to nonaffiliated third parties ''as permitted by law'' to describe disclosures made pursuant to one of the exceptions. Others agreed with the proposed flexibility to allow a disclosure to be based on current and contemplated information sharing. In addition, the Commission received may requests for model forms of privacy notices. In light of these comments, the Commission has adopted proposed § 313.6 with changes as discussed above, plus stylistic changes to the material in § 313.6 that are intended to make the rule easier to read, and added the sample clauses in Appendix A.

Section 313.7 Form of Opt Out Notice to Consumers; Opt Out Methods

Paragraph (a) of proposed § 313.8 required that any opt out notice provided by a financial institution be clear and conspicuous and accurately explain the right to opt out. The

[34] *See, e.g.*, remarks of Sen. Gramm (noting that the privacy bill contains ''for the first time a full disclosure requirement. It requires every bank in America, when you open your account to tell you precisely what their policy is: Do they share personal financial information within the bank? Do they share it outside the bank?''), 145 Cong. Rec. S13786 (daily ed. Nov. 3, 1999); remarks of Sen. Hagel, *id.* at S13876 (''Financial institutions would be required to disclose their privacy policies to their customers on a timely basis. If customers do not believe adequate protections exist at their institution, they can take their business elsewhere.'').

proposed rule also required a financial institution to provide the consumer with a reasonable means by which to opt out, required a financial institution to honor an opt out election as soon as reasonably practicable, and stated that an opt out election survived until revoked by the consumer. The Commission received several comments in response to each of these provisions, addressing the application of these rules to joint accounts, the means by which an opt out right may be exercised, duration of an opt out, the level of detail required in the opt out notice, and the time by which an opt out election must be honored. These points are addressed below.

Joint accounts. Most of the commenters on this issue stated that a financial institution should have the option of providing one notice per account, regardless of the number of persons on the account. The Commission has added a new § 313.7(d) to address this issue. Under the final rule, a financial institution has the option of providing only one initial, annual, and opt out notice per account. However, if one or more of the joint account holders requests separate notices, the financial institution must honor that request. Even in instances where only one notice is provided, any of the accountholders must have the right to opt out. The final rule requires a financial institution to state in the opt out notice provided to a joint accountholder whether the institution will consider an opt out by a joint accountholder as an opt out by all of the associated accountholders or whether each accountholder is permitted to opt out separately.

Means of opting out. Another issue addressed by many commenters concerned the means by which consumers may opt out. Several suggested that a financial institution, after having provided reasonable means of opting out, should be able to require consumers to use those means exclusively. The Commission recognizes that a financial institution may not have trained personnel or systems in place to handle opt out elections at each point of contact between a consumer and financial institution. Assuming a financial institution offers one or more of the opt out means provided in the examples in the final rule or a means of opting out that is comparably convenient for a consumer, the institution may require consumers to opt out in accordance with those means and choose not to honor opt out elections communicated to the institution through alternative means. A new paragraph (iv) has been added to § 313.7(a)(2)(iv) to reflect this. However, as stated in § 313.7(a)(2)(iii)(A), a financial institution may not require a consumer to write his or her own letter in order to opt out.

Several commenters supported the alternative ways in which financial institutions could provide for consumers to opt out, especially the toll-free number set forth in § 313.8(a)(2)(ii)(D) in the Commission's proposal that was not included in the other Agencies' proposed rule. The Commission has retained that example in § 313.7(a)(2)(ii)(D) of the final rule, and the other Agencies have added the toll-free telephone number to their lists of examples. The Commission also received numerous comments indicating that one of the proposal's means of opting out, providing a self-addressed stamped envelope with a detachable card, was too burdensome. The Commission has, therefore, revised that example to provide for a reply form that contains the relevant address to facilitate the consumers ability to return it.

Duration of opt out. Several commenters questioned the practicality of the rule concerning duration of an opt out, as provided in § 313.8(e) of the proposal. These commenters noted that, under the proposal, a financial institution would be required to keep track of opt out elections forever. To illustrate their point, the commenters posited the example of a person who opts out during the course of establishing a customer relationship with a financial institution, terminates that relationship, and then establishes another customer relationship several years later, perhaps under a different name or with someone on a joint account. The commenters suggested that it would be more appropriate in these circumstances to treat the opt out election made in connection with the first relationship as applying solely to that relationship.

The Commission agrees. Thus, under the final rule, a financial institution is not required to treat an opt out election made by a customer in connection with a prior customer relationship as applying solely to the nonpublic personal information that the financial institution collected during, or related to, that relationship. That opt out will continue until the customer revokes it. However, if the customer relationship terminates and a new one is established at a later point, the financial institution must then provide a new opt out notice to the customer in connection with the new relationship and any prior opt out election does not apply to the new relationship.

Level of detail required in opt out notice. A few commenters expressed concern about the level of detail they perceived the proposed rule to require in an opt out notice. These commenters interpreted the statement in proposed § 313.8(a)(2) that a financial institution ''provides adequate notice . . . if [the institution] identifies all of the categories of nonpublic personal information that [the institution] discloses or reserves the right to disclose to nonaffiliated third parties as described in [§ 313.6]'' as requiring a more detailed disclosure of categories of nonpublic personal information and nonaffiliated third parties than is required in the initial and annual notices.

The Commission did not intend this result, and specifically referred to § 313.6 in the proposed opt out provision to address precisely the concern raised by these commenters. The disclosures in the initial and annual notices of the categories of nonpublic personal information being disclosed and the categories of nonaffiliated third parties to whom the information is disclosed will suffice for purposes of the opt out notices as well. If the opt out notice is a part of the same document that contains the disclosures that must be included in the initial notice, then the financial institution is not required to restate the same information in the opt out notice. In this instance, the rule requires only that the categories of nonpublic personal information the institution intends to share and the categories of nonaffiliated third parties with whom it will share are clearly disclosed to the consumer when the opt out and privacy notices are read together.

One commenter suggested that, while a financial institution should have the option of providing an opt out notice that is sufficiently broad to cover anticipated disclosures, the financial institution also should be permitted to provide a customer who already has opted out with a new opt out notice in connection with a new financial product or service and, if the consumer does not opt out a second time, be free to disclose nonpublic personal information obtained in connection with that financial product or service to nonaffiliated third parties. The Commission believes that a financial institution should be permitted the flexibility to provide opt out notices that are either clearly limited to specific types of nonpublic personal information and types of nonaffiliated third parties, or that are more broadly worded to anticipate future disclosure plans. However, if a consumer opts out after

receiving an opt out notice from a financial institution that is broad enough to cover the new type of information sharing desired by that institution, the failure of the consumer to opt out again does not revoke the earlier opt out election.

Time by which opt out must be honored. Under the proposal, a financial institution is directed to comply with an opt out election ''as soon as reasonably practicable.'' A large number of comments asked the Commission to clarify in the final rule how long a financial institution has after receiving an opt out election to cease disclosing nonpublic personal information to nonaffiliated third parties. Suggestions for a more precise standard ranged from mandating that a financial institution stop disclosing information immediately to a mandatory cessation within several months of receiving the opt out. As was the case with other suggestions for bright-line standards in different contexts, the Commission believes that it is appropriate to retain a more general rule in light of the wide range of practices throughout the various financial institutions within its jurisdiction. A potential drawback of a more prescriptive rule is that an institution might use the standard as a safe harbor in all instances and thus fail to honor an opt out election as early as it is otherwise capable of doing. Another drawback is that a standard that is set in light of current industry practices and capabilities may become outmoded as advances in technology increase efficiency. The Commission therefore declines to adopt a more rigid standard and instead retains the rule as set out in § 313.7(e) of the final rule.

For the reasons stated above, the Commission adopts, in § 313.7, the rule governing the form of opt out notices and methods of opting out as discussed above. This section contains other stylistic changes to what was proposed in order to make the final rule easier to read.

Section 313.8 Revised Privacy Notices

The proposed rule, in § 313.8(c) (''Notice of change in terms''), prohibited a financial institution (directly, or through its affiliates) from disclosing nonpublic personal information about its consumers to nonaffiliated third parties unless the institution first provided a copy of its privacy notice and opt out notice. The proposal also required that these notices be accurate when given. Thus, if an institution wants to disclose nonpublic personal information in a way that is not accurately described in its notices, the institution would be required under the proposed rule to provide new notices before making the disclosure in question.

The only comments relating to these requirements received by the Commission posited that a revised notice should be required only upon material changes. Section 313.8(a)(i) addresses this point—no new notice is required if the original notice ''accurately describes'' the institution's policies. Accordingly, the Commission adopts the rule as proposed, but places the relevant provisions in a separate section (§ 313.8, ''Revised privacy notices'') in the final rule for emphasis. The final rule sets out examples in § 313.8(b) of when a new notice would, and would not, be required.

Section 313.9 Delivering Privacy and Opt Out Notices

The proposed rules governing delivery of initial, annual, and opt out notices were set out in proposed §§ 313.4(d), 313.5(b), and 313.8(b), respectively. Given the substantial similarities between the three sets of rules, the Commission has decided to combine the rules in one section in order to make it easier for the reader. Accordingly, the final rule states these rules in § 313.9.

The general rule requires that notices be provided in a manner so that each consumer can reasonably be expected to receive actual notice in writing, or, if the consumer agrees, electronically. The Commission received a number of comments on the various provisions governing delivery, as discussed below.

Posting initial notices on a web site. A few commenters suggested that a financial institution be allowed to deliver initial notices simply by posting its notice on the institution's web site. Some of them criticized the example in proposed § 313.4(d)(5)(C) that required the consumer to acknowledge receipt of an electronic communication as tantamount to an ''opt-in'' provision; conversely, at least one consumer representative vigorously contended that it was essential that the consumer affirmatively respond in this situation because computer literacy cannot be presumed from the use of a web site.

There will be instances when a notice on a web site may be delivered in a way that will enable the financial institution to reasonably expect that the consumer will receive it. The final rule retains, as an example of one way to comply with the rule, the posting of a notice on a web site and requiring a consumer to acknowledge receipt of the notice as a step in the process of obtaining a financial product or service. *See* § 313.9(b)(1)(iii). However, the mere posting of a notice on a web site would not be sufficient in all cases for the financial institution to reasonably expect its consumers to receive the notice. Accordingly, the Commission does not view the limited acknowledgment of receipt in this context as equivalent to an opt in requirement.

Posting annual notices on a web site. Several commenters requested that a privacy notice posted by a financial institution on its web site be deemed to satisfy the annual notice requirement, at least for customers who agree to receive notices on the institution's web site. The final rule contains a new § 313.9(c)(i) to clarify that a financial institution may reasonably expect that a customer who uses the institution's web site to access financial products or services will receive actual notice if the customer has agreed to accept notices at the institution's web site and the financial institution posts a current notice of its privacy policies and practices continuously and in a clear and conspicuous manner on the web site.

The Commission views it as appropriate to post the annual notice on the web site only where the customer is in a relationship with the financial institution that is conducted almost entirely at the web site and where the customer has explicitly agreed to receive all of its notices and financial information at the web site. Moreover, the financial institution must position any link or links to the privacy policy such that they are evident to the customer wherever the customer may go on the web site to conduct transactions or obtain information. In those circumstances, the Commission agrees that it is appropriate to provide annual notices in this way for customers who conduct transactions electronically and agree to accept notices on a web site. This will reduce burden on financial institutions while ensuring that customers who transact business electronically will have access to institutions' privacy policies and practices.

Disclosures to customers requesting no communication. Several commenters suggested the Commission clarify in the final rule how the disclosure obligations may be met in the case of a customer who requests that the institution refrain from sending information about the customer's relationship. These commenters stated that, in this case, the customer's request should be honored.

The Commission agrees. When a customer provides explicit instructions for a financial institution not to communicate with that customer, the

Commission believes that the request should be honored. The final rule clarifies, in § 313.9(c)(ii), that financial institutions need not send notices to a customer who requests no communication, provided that a notice is available upon request.

Reaccessing a notice. A few commenters stated that the requirement that a privacy policy be provided in a way that enables a customer to either retain or reaccess the notice should clarify that the rule obligates a financial institution to make available only the privacy policy currently in effect. These commenters were concerned about the potential for confusion and the burden stemming from a rule that would require a financial institution to make available every version of its privacy policies. The Commission agrees that it is appropriate to require only that the current privacy policy be made available to someone seeking to obtain it after having received the initial notice, and has revised the final rule accordingly in § 313.9(e)(2)(iii).

Joint notices. Other commenters requested that the rule clarify that the privacy policies and practices of several different affiliated financial institutions may be described on a single notice. Further, commenters requested that the final rule address whether affiliated financial institutions, each of whom has a customer relationship with the same consumer, may elect to send only one notice to the consumer on behalf of all of the affiliates covered by the notice and have that one notice satisfy the disclosure obligations under § 313.4 of each affiliate. Financial institutions should be able to combine initial disclosures in one document. The Commission also believes that it is appropriate to permit financial institutions that prepare a combined initial or annual notice to give, on a collective basis, a consumer only one copy of the notice. The final rule reflects this flexibility, in § 313.9(f). The notice must be accurate for all financial institutions using the notice, and must identify by name each of the institutions. The Commission also notes that financial institutions that provide one combined notice must be capable of keeping track of whether a consumer has opted out in order to ensure that disclosures are made in accordance with whatever opt out instructions a consumer provides after having received the joint notice.

Section 313.10 Limits on Disclosure of Nonpublic Personal Information to Nonaffiliated Third Parties

Section 502(a) of the G-L-B Act generally prohibits a financial institution, directly or through its affiliates, from sharing nonpublic personal information about a consumer with a nonaffiliated third party unless the institution provides the consumer with a notice of the institution's privacy policies and practices. Section 502(b) further requires that the financial institution provide the consumer with a clear and conspicuous notice that the consumer's nonpublic personal information may be disclosed to nonaffiliated third parties, that the consumer be given an opportunity to opt out of that disclosure, and that the consumer be informed of how to opt out. Section 313.7 of the proposed rule implemented these provisions by requiring a financial institution to give the consumer the initial notice required by § 313.4, the opt out notice required by § 313.8, and a reasonable opportunity to opt out.

Most of the comments addressing these requirements focused on the question of what is a reasonable opportunity to opt out. Suggestions ranged from a financial institution having the right to begin sharing information immediately (when the opt out and initial notices are provided as part of a transaction being conducted electronically, such as might be the case in an ATM transaction) up to a mandatory delay of 120 days from the time the notices are provided.

The wide variety of suggestions underscores the appropriateness of a more general test that avoids setting a mandatory waiting period applicable in all cases. For isolated transactions where a financial institution intends to disclose nonpublic personal information that it obtains through an electronic transaction and the consumer is provided a convenient means of opting out as part of the transaction, it would be reasonable not to force the financial institution to wait a set period of time before sharing the information. Thus, the example in § 313.10(a)(3)(iii) provides flexibility. For other opt out notices that are provided by mail, the Commission believes it is appropriate to allow the consumer additional time. In these latter instances, the Commission considers it reasonable to permit the consumer to opt out by mailing back a form, by calling a toll-free number, or by any other reasonable means within 30 days from the date the opt out notice was mailed. *See* § 313.10(a)(3)(i). The final rule also provides an example of a reasonable opportunity for opting out in connection with accounts opened on-line. *See* § 313.10(a)(3)(ii). However, rather than try to anticipate every scenario and establish a time frame that would accommodate each, the rule simply provides that the consumer must be given a reasonable opportunity to opt out and then provide a few illustrative examples of what would be reasonable in different contexts.

Other comments pointed out that proposed § 313.7(a)(3)(i), which is § 313.10(a)(3)(i) of the final rule, inappropriately implied that the opportunity to opt out by mail is available only when a consumer has a customer relationship with the financial institution. The final rule deletes the reference to a customer relationship in that section to avoid that implication.

Section 313.11 Limits on Redisclosure and Reuse of Information

Section 502(c) of the G-L-B Act provides that a nonaffiliated third party that receives nonpublic personal information from a financial institution shall not, directly or indirectly through an affiliate, disclose the information to any person that is not affiliated with both the financial institution and the third party, unless the disclosure would be lawful if made directly by the financial institution. The proposed rule implemented section 502(c) by imposing limits on redisclosure that apply both to a financial institution that receives information from a nonaffiliated financial institution and to any nonaffiliated third party that receives nonpublic personal information from a financial institution. The proposed rule also imposed limits on the ability of financial institutions and nonaffiliated third parties to reuse nonpublic personal information they receive. As noted in the preamble to the proposed rule, sections 502(b)(2) and 502(e) permit disclosures of nonpublic personal information for specific purposes. The Commission sought comment on whether the final rule should limit the ability of an entity that receives nonpublic personal information pursuant to an exception to use that information only for the purpose of that exception. The Commission also sought comment on what the term ''lawful'' means in the context of section 502(c), and whether a recipient of nonpublic personal information could ''lawfully'' disclose information if the disclosure complied with a notice provided by the institution that made the disclosure initially. Finally, the Commission invited comment on whether the rule should require a financial institution that discloses nonpublic personal information to a nonaffiliated third party to develop policies and procedures to ensure that the third party complies with the limits on redisclosure of that information.

The Commission received many comments in response to this proposed section. A few opined that the Commission would exceed its rulemaking authority if the final rule were to retain the limits on reuse of information, given that section 502(c) expressly addresses only redisclosures and not reuse. Most comments concerning proposed § 313.12 stated that financial institutions should not have to monitor compliance with the redisclosure and reuse provisions of the rule, although these commenters said that financial institutions typically will contractually limit the recipient's ability to reuse information for purposes other than those for which the information was disclosed. The Commission also received comments from consumer reporting agencies, individual reference services, private investigators, and direct marketers stating that consumer reporting agencies should be able to continue their practice of selling ''credit header'' information that they obtain from financial institutions, as well as some comments stating that the Commission should clarify that the rules prohibit the continued distribution of such information by consumer reporting agencies. These issues are addressed below.

Limits on reuse. Those critical of imposing limits on reuse believe that Congress, by addressing limits on redisclosures in section 502(c), provided the only limits that may be imposed on what a recipient of nonpublic personal information can do with that information. The Commission disagrees. Section 502(c) is silent on the question of reuse, making it necessary to look to the overall purposes of the statute to determine whether the Commission should impose limits on the ability of nonaffiliated third parties to reuse nonpublic personal information that they receive from a financial institution. The Act makes it appropriate to impose limits on reuse, depending on whether the information was obtained pursuant to one of the exceptions in section 502(e) of the G-L-B Act (as implemented by §§ 313.14 and 313.15 of the final rule).

When disclosures are made to nonaffiliated third parties in connection with one of the purposes set out in section 502(e), those disclosures are exempt from the notice and opt out protections altogether. A customer has no right to prohibit those disclosures or even to know more than that the disclosures are being made ''as permitted by law.'' A consumer who does not establish a customer relationship is not even put on notice that the disclosures are made as permitted by law, because the consumer is not entitled to any privacy or opt out notice. The only protection afforded by the statute for disclosures made under section 502(e) is the limited nature of the exceptions. It would be inappropriate to undermine the key privacy requirements of the Act that ensure a consumer can generally control the disclosure of his or her nonpublic personal information by allowing the recipient of nonpublic personal information under the section 502(e) exception to reuse the information for any purpose, including marketing.

By contrast, when a consumer decides not to opt out after being given adequate notices and the opportunity to do so, that consumer has made a decision to permit the sharing of his or her nonpublic personal information with the categories of entities identified in the financial institution's notices. The consumer's primary protection in the case of a disclosure falling outside the section 502(e) exceptions comes from receiving the mandatory disclosures and the right to opt out. The statute provides only the additional protection in section 502(c), restricting a recipient's ability to redisclose information to entities that are not affiliated with either the recipient or the financial institution making the disclosure initially. Thus, if a consumer permits a financial institution to disclose nonpublic personal information to the categories of nonaffiliated third parties that are described in the institution's notices, recipients of that nonpublic personal information appear authorized under the statute to make disclosures that comply with those notices.

To implement this statutory scheme, the Commission has retained a limit on reuse in addition to the limit on redisclosures. The limits on redisclosure and reuse that apply to recipients of information and their affiliates will vary, depending on whether the information was provided pursuant to one of the section 502(e) exceptions.

For nonpublic personal information provided pursuant to section 502(e), a financial institution receiving the information may disclose the information to its affiliates or to affiliates of the financial institution from which the information was received. It may also disclose and use the information pursuant to an exception in §§ 313.14 or 313.15 in the ordinary course of business to carry out the activity covered by the exception under which the institution received the information. Therefore, the financial institution's affiliates may disclose and use the information, but only to the extent permissible for the financial institution under those exceptions.

For nonpublic personal information provided *outside* one of the section 502(e) exceptions (*i.e.*, where a customer or consumer has not opted out), the financial institution receiving the information may disclose the information to its affiliates or to the affiliates of the financial institution that made the initial disclosure. It may also disclose the information to any other person, if the disclosure would be lawful if made directly by the financial institution from which the information was received. This would enable the receiving institution to redisclose information pursuant to one of the section 502(e) exceptions. It also would permit the receiving institution to redisclose information in accordance with the opt out and privacy notices given by the institution making the initial disclosures, as limited by any opt out elections received by that institution. The affiliates of a financial institution that receives nonpublic personal information may disclose only to the extent that the financial institution may disclose the information.

These same general rules apply to a *non-financial institution* third party that receives nonpublic personal information from a financial institution. Thus, the third party receiving the information pursuant to one of the section 502(e) exceptions may disclose the information to its affiliates or to the affiliates of the financial institution that made the disclosure. The third party also may disclose and use the information pursuant to one of the section 502(e) exceptions as noted in the rule. The affiliates of the third party may disclose and use the information only to the extent permissible for the third party. If the third party receives the information from a financial institution outside one of the section 502(e) exceptions, the third party may disclose to its affiliates or to the affiliates of the financial institution. It may also disclose to any other person if the disclosure would be lawful if made by the financial institution. The third party's affiliates may disclose and use the information to the same extent permissible for the third party.

To summarize, in cases where an entity receives information outside of one of the section 502(e) exceptions, that entity will in essence ''step into the shoes'' of the financial institution that made the initial disclosures. Thus, if the financial institution made the initial disclosures after representing to its consumers that it had carefully screened the entities to whom it intended to

disclose the information, the receiving entity must be able to comply with those representations. Otherwise, the subsequent disclosure by the receiving entity would not be in accordance with the notices given to consumers and would not, therefore, be lawful. Even if such representations do not prevent the recipient from redisclosing the information, the recipient's ability to redisclose will be limited by whatever opt out instructions were given to the institution making the initial disclosures and by whatever new opt out instructions are given after the initial disclosure. The receiving entity, therefore, must have procedures in place to continually monitor the status of who opts out and to what extent. Given these practical limitations on the ability of a recipient to disclose pursuant to another institution's privacy and opt out notices, redisclosure of information is most likely to arise under one of the section 502(e) exceptions (as implemented by §§ 313.14 and 313.15 of the final rule).

Monitoring third parties. The final rule does not impose a general duty on financial institutions to monitor third parties' use of nonpublic personal information provided by the institutions. Obligations to do so may arise in other contexts, however. For instance, some of the commenters who requested that the Commission not impose such a duty stated that they have contracts in place that limit what the recipient may do with the information. Also, the limits on reuse as stated in the final rule provide a basis for an action to be brought against an entity that violates those limits.

Redisclosure by consumer reporting agencies. Comments regarding the availability of credit header information [35] from consumer reporting agencies addressed not only the reuse and redisclosure provisions, but also the definition of nonpublic personal information (*see* § 313.3(n, o, p) above), the exception in § 313.15(a)(5), and the operation of the Fair Credit Reporting Act (*see* § 313.16 below). For clarity, the Commission addresses the credit header issue here, with reference as appropriate to other provisions of the final rule.

The definition of nonpublic personal information dictates that all of the information a financial institution provides to a consumer reporting agency is nonpublic personal information: ''Any list, description or other grouping of consumers (*and publicly available information pertaining to them*) that is derived using any personally identifiable financial information * * *.'' (§ 313.3(n)(1)(ii)(emphasis added).) The financial institution is permitted under § 313.15(a)(5) to disclose this nonpublic personal information, without giving the consumer notice and the opportunity to opt out, ''[t]o a consumer reporting agency * * *.'' That same exception states that the notice and opt out provisions do not apply to nonpublic personal information ''from a consumer report reported by a consumer reporting agency.''

The Commission recognizes that § 313.15(a)(5) permits the continuation of the traditional consumer reporting business, whereby financial institutions report information about their consumers to the consumer reporting agencies and the consumer reporting agencies, in turn, disclose that information in the form of consumer reports to those who have a permissible purpose to obtain them. Despite a contrary position expressed by some commenters, this exception does not allow consumer reporting agencies to redisclose the nonpublic personal information it receives from financial institutions other than in the form of a consumer report. Therefore, the exception does not operate to allow the disclosure of credit header information to individual reference services, direct marketers, or any other party that does not have a permissible purpose to obtain that information as part of a consumer report.[36]

Disclosure by a consumer reporting agency of the nonpublic personal information it receives from a financial institution pursuant to the exception, other than in the form of a consumer report, is governed by the limitations on reuse and redisclosure in § 313.11, discussed above in ''Limits on reuse.'' Those limitations do not permit consumer reporting agencies to disclose credit header information that they received from financial institutions to nonaffiliated third parties. Some commenters suggested that the information loses its status as ''nonpublic personal information'' when the consumer reporting agencies combine it with other information in their databases. The Commission does not agree. The information is disclosed to the consumer reporting agencies as nonpublic personal information and it retains that status regardless of how the consumer reporting agency stores or rediscloses that data.

Several commenters stated that the Fair Credit Reporting Act operates to allow consumer reporting agencies to disclose credit header information and, therefore, any prohibition on the sale of credit header information violates section 506 of the G–L–B Act, which states that ''nothing in [Title V of the G-L-B Act] shall be construed to modify, limit, or supercede the operation of the [FCRA].'' The Commission does not agree. To the extent credit header information is not a consumer report, it is not regulated by the FCRA and a prohibition on its disclosure by a consumer reporting agency consistent with the statutory scheme of the G-L-B Act in no way modifies, limits or supercedes the operation of the FCRA.[37]

At least one commenter requested that the Commission make use of the authority granted to it under section 504(b) of the G-L-B Act to provide for an exception to the reuse and redisclosure limitations that would allow consumer reporting agencies to sell credit header information. The Commission does not believe that such an exception is consistent with the privacy provisions of the Act, which function to protect a consumer's nonpublic personal information from widespread distribution without notice and the opportunity for the consumer to opt out. An exception that allows a consumer reporting agency to redisclose that information where there has been no notice to the consumer and no opportunity for the consumer to direct that the information not be disclosed works at cross purposes with the Act. The Commission, therefore, declines to adopt such an exception.

If consumer reporting agencies receive credit header information from financial institutions outside of an exception, the limitations on reuse and redisclosure may allow them to continue to sell that information. This could occur if the originating financial institutions disclose in their privacy policies that they share consumers' nonpublic personal information with consumer reporting agencies, and provide consumers with the opportunity to opt out. Then, like any other nonaffiliated third party that receives information outside of an exception, the consumer

[35] ''Credit header'' information was traditionally defined to include identifying information such as name, address, telephone number, social security number, mother's maiden name, and age. However, the Commission's recent decision in *In re Trans Union,* Docket No. 9255 (Feb. 10, 2000), *appeal docketed,* No. 00–1141 (D.C. Cir. Apr. 4, 2000), determined that age is a ''consumer report'' and can be disclosed only pursuant to a permissible purpose under Section 604 of the Fair Credit Reporting Act.

[36] Section 608 of the Fair Credit Reporting Act does allow consumer reporting agencies to furnish a consumer's name, address, former addresses, places of employment, and former places of employment to a governmental agency.

[37] To the extent that previously-considered credit header information is now deemed consumer report information (*i.e.,* age), the FCRA provides requirements and protections in addition to those provided under the G-L-B Act.

reporting agency can redisclose that information consistent with the originating financial institutions' privacy policies and subject to applicable consumer opt out directions.

Section 313.12 Limits on Sharing Account Number Information for Marketing Purposes.

Section 502(d) of the G-L-B Act prohibits a financial institution from disclosing, ''other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.'' Proposed § 313.13 applied this statutory prohibition to disclosures made directly or indirectly by a financial institution and sought comment on whether one or more exceptions to the flat prohibition should be created.

The Commission received many comments from people who suggested that various exceptions be created, as well as people who believe that a flat prohibition is necessary to protect consumers from unscrupulous practices. After considering the suggestions from all of the commenters addressing this issue, the Commission has decided, pursuant to its authority under 504(b), to modify proposed § 313.13 by (a) adding two exceptions that allow financial institutions to engage in legitimate, routine business practices and that are unlikely to pose a significant potential for abuse and (b) clarifying that the prohibition does not apply in two circumstances frequently mentioned in the comments. These exceptions and clarifications are discussed below.

Disclosures to a financial institution's agent or service provider. Many financial institutions noted that they use agents or service providers to conduct marketing on the institution's behalf. This might occur, for instance, when a mortgage lender instructs a service provider that assists in the delivery of monthly statements to include a ''statement stuffer'' with the statement informing consumers about a financial product or service offered by the institution. The Commission recognizes the need to disclose account numbers in this instance, and believe that there is little risk to the consumer presented by such disclosure.

Similarly, the Commission recognizes that a financial institution may use agents to market the institution's own financial products and services. Commenters advocating that the final rule exclude disclosures to agents stated that the agents effectively act as the financial institution in the marketing of the institution's financial products and services. These commenters suggested that there was no more reason to preclude sharing the account numbers with an agent hired to market the institution's financial products and services than there would be to preclude sharing between two departments of the same institution. The Commission is concerned, however, about the possibility of transactions being consummated by a financial institution's agent who may be engaging in practices contrary to the institution's instructions. While the Commission recognizes that a financial institution frequently will use agents to assist it in marketing its products, a consumer's protections are potentially eroded by allowing agents to have access to a consumer's account. Accordingly, an exception in § 313.12(b)(1) will permit disclosures of account numbers by a financial institution to an agent for the purpose of marketing the financial institution's financial product or services, but has qualified that exception by stating that the agent has no authority to make charges to the account.

Private label credit cards and affinity programs. Many commenters stated that the final rule should not prevent the disclosure of account numbers in the situation where a consumer chooses to participate in a private label credit card program or other affinity program. Under these programs, a consumer typically will be offered certain benefits, often by a retail merchant, in return for using a credit card that is issued by a particular financial institution. The commenters suggested that, in the example of an affinity program, the consumer understands the need for the merchant and financial institution to share the consumer's account number. The Commission agrees that this type of disclosure is appropriate and does not create a significant risk to the consumer. Accordingly, § 313.12(b)(2) has been added to the final rule to exclude the sharing of account numbers where the participants are identified to the consumer at the time the consumer enters into the program.

Encrypted numbers. Many commenters urged the Commission to exercise its exemptive authority to permit the transmission of account numbers in encrypted form. Several commenters noted that encrypted account numbers and other internal identifiers of an account are frequently used to ensure that a consumer's instructions are properly executed and that the inability to continue using these internal identifiers would increase the likelihood of errors in processing a consumer's instructions. These commenters also point out that if internal identifiers may not be used, a consumer would need to provide an account number in order to ensure proper handling of a request, which would expose the consumer to a greater risk than would the use of an internal tracking system that preserves the confidentiality of a number that may be used to access the account.

The Commission believes an encrypted account number without the key is something different from the number itself and thus falls outside the prohibition in section 502(d). In essence, it operates as an identifier attached to an account for internal tracking purposes only. The statute, by contrast, focuses on numbers that provide *access* to an account. Without the key to decrypt an account number, an encrypted number does not permit someone to access an account.

In light of the statutory focus on access numbers, and given the demonstrated need to be able to identify which account a financial institution should debit or credit in connection with a transaction, the Commission has included a clarification in § 313.12(c)(1) of the final rule stating that an account number, or similar form of access number or access code, does not include a number or code in an encrypted number form, as long as the financial institution does not provide the recipient with the means to decrypt the number. Consumers will be adequately protected by disclosures of encrypted account numbers that do not enable the recipient to access the consumer's account.

Definition of ''transaction account.'' Several commenters suggested that the final rule clarify that accounts to which no charge may be posted are not covered by the prohibition against disclosing account numbers. These commenters frequently cited mortgage loan accounts as typical of those that should fall outside the scope of the prohibition. The Commission agrees with the principle behind these suggestions. However, there have been instances in which a borrower's monthly payments on a mortgage loan have been increased in connection with the marketing of a financial product or service without the borrower's knowledge or permission. Accordingly, the final rule clarifies in § 313.12(c)(2) that a transaction account is an account, other than a deposit account or a credit card account, to which third parties can initiate charges.

If it would be possible, for instance, for a third party marketer to initiate a charge to a mortgage loan account, then the final rule would prohibit the disclosure of that account number to the marketer.

Section 313.13 Exception To Opt Out Requirements for Service Providers and Joint Marketing

Section 502(b) of the G-L-B Act creates an exception to the opt out rule for the disclosure of information to a nonaffiliated third party for use by the third party to perform services for, or functions on behalf of, the financial institution, including the marketing of the financial institution's own products or services or financial products or services offered pursuant to a joint agreement between two or more financial institutions. A consumer will not have the right to opt out of disclosing nonpublic personal information about the consumer to nonaffiliated third parties under these circumstances, if the financial institution ''fully discloses'' to the consumer that it will provide this information to the nonaffiliated third party before the information is shared and enters into a contract with the third party that requires the third party to maintain the confidentiality of the information. As noted in the proposed rule, this contract should be designed to ensure that the third party (a) will maintain the confidentiality of the information at least to the same extent as is required for the financial institution that discloses it, and (b) will use the information solely for the purposes for which the information is disclosed or as otherwise permitted by §§ 313.10 and 313.11 of the proposed rule. The Commission invited comment on whether the statute would prohibit the sharing of aggregate data without personal identifiers and whether additional requirements should be imposed on the agreements to address, for instance, reputation risk and legal risk for a financial institution entering into such an agreement.

The majority of the comments on this exception expressed concern that routine servicing agreements between a financial institution and, for instance, a loan servicer would be subject to the requirements of proposed § 313.9, which appears as § 313.13 in the final rule. These commenters consistently pointed out that section 502(e) of the G-L-B Act contains several exceptions for the sharing of information by a financial institution that is necessary to permit a third party to perform services for a financial institution. The commenters requested clarification that disclosures made pursuant to one of the section 502(e) exceptions are not subject to the requirements imposed on disclosures made pursuant to section 502(b)(2) of the G-L-B Act. The Commission agrees that when a disclosure may be made under section 502(e), the Act permits that disclosure without first complying with the requirements of section 502(b)(2).

A related issue is whether a financial institution must satisfy the disclosure obligations of section 502(b)(2) and have a confidentiality agreement in the case of a service provider that is performing an activity governed by section 502(b)(2) (*i.e.,* those that are not covered by one of the section 502(e) exceptions). Several commenters maintained that those requirements apply only to joint marketing agreements and that it is illogical to impose a set of requirements on disclosures to the section 502(b)(2) service providers when no such requirements are imposed on the section 502(e) service providers. The Commission believes, however, that a plain reading of section 502(b)(2) leads to that result.[38] The Commission reads the phrase ''if the financial institution fully discloses * * *'' as used in section 502(b)(2) as modifying the phrase ''[t]his subsection shall not prevent a financial institution from providing nonpublic personal information to a nonaffiliated third party to perform services for or functions on behalf of the financial institution, * * *'' The Commission thus has concluded that any disclosure to a service provider not covered by section 502(e) must satisfy the disclosure and written contract requirements of section 502(b)(2).

Several other commenters addressed the question of whether the rule should include safeguards beyond those provided by the statute to protect a financial institution from the risks that can arise from agreements with third parties. Most suggested that safety and soundness concerns were more appropriately addressed in a forum other than a rule designed to protect consumers' financial privacy. Others opined that financial institutions did not need the rule to mandate certain protections on their behalf. The Commission has concluded that the protections set out in the statute, as implemented by § 313.13(a)(1)(ii), are adequate for purposes of the privacy rule. Those protections require a financial institution to provide the initial notice required by § 313.4 of the final rule as well as enter into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the financial institution disclosed the information, including use under an exception in §§ 313.14 or 313.15 in the ordinary course of business to carry out those purposes. These limitations will preclude recipients from sharing a consumer's nonpublic personal information pursuant to a chain of third party joint marketing agreements.

Several commenters asked whether a financial institution would have to modify existing contracts with third parties to comply with the rule. The Commission believes that a balance must be struck that minimizes interference with existing contracts while preventing evasions of the regulation. To achieve these goals, the final rule states, in § 313.18(c), that contracts in effect as of July 1, 2000 must be brought into compliance with the provisions of § 313.13 by July 1, 2002. For the reasons expressed above, the Commission has adopted the provisions that were set out in § 313.9 of the proposal, with the changes noted above, as § 313.13 of the final rule.

Section 313.14 Exceptions to Notice and Opt Out Requirements for Processing and Servicing Transactions

As previously discussed, section 502(e) of the G-L-B Act creates exceptions to the requirements that apply to the disclosure of nonpublic personal information to nonaffiliated third parties. Paragraph (1) of that section sets out certain exceptions for disclosures made, generally speaking, in connection with the administration, processing, servicing, and sale of a consumer's account. Proposed § 313.10 implemented those exceptions by restating them with only stylistic changes that were intended to make the exceptions easier to read. The preamble to that proposed section noted that the exceptions set out in proposed § 313.10 (as well as the exceptions set out in § 313.11 of the proposal) do not affect a financial institution's obligation to provide initial notices of its privacy policies and practices prior to the time it establishes a customer relationship and annual notices thereafter.

[38] Section 502(b)(2) states, in relevant part, that the opt out provision: ''shall not prevent a financial institution from providing nonpublic personal information to a nonaffiliated third party to perform services for or functions on behalf of the financial institution, including the marketing of the financial institution's own products or services, or financial products or services offered pursuant to joint agreements between two or more financial institutions that comply with the requirements imposed by the regulations prescribed under section 504, if the financial institution fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information.

The Commission received several comments from institutions pointing out that, by deleting the statutory phrase ''in connection with'' from the exceptions for information shared (a) to service or process a financial product or service requested by the consumer or (b) to maintain or service a customer account, the Commission narrowed the application of the exception. The Commission did not intend this result and has changed the final rule accordingly. *See* § 313.14(a).

Several other commenters requested that the final rule specifically state that certain services, such as those provided by attorneys, appraisers, financial planners, and debt collectors (as appropriate), are ''necessary'' to effect, administer, or enforce a transaction, as that term is used in paragraph (a) and defined in paragraph (b) of proposed § 313.10. Others cited examples of entities seeking to verify funds availability or obtain loan payoff information as instances where a disclosure would fall within the exceptions described in proposed § 313.10. The Commission believes that disclosures to these types of professionals and under the circumstances posited by the commenters may be necessary to effect, administer, or enforce a transaction in a given situation. However, the Commission has not listed specific types of disclosures in the regulation as necessarily falling within the scope of the exception because such a general statement could be applied inappropriately to shelter disclosures that, in fact, are not necessary to effect, administer, or enforce a transaction.

Other commenters suggested that the final rule clarify, in situations where a financial institution uses an agent to provide services to a consumer, that the consumer need not have directly requested or authorized the service provider to provide the financial product or service but may request it from the principal instead. The Commission agrees that the communication may be between the consumer and the service provider and notes that the rule governing agents as set out in the definition of ''consumer'' above, provides the flexibility sought by the commenters. Briefly stated, an individual is not a consumer of an entity that is acting as agent for another financial institution in connection with that financial institution's providing a financial product or service to the consumer.

Section 313.15 Other Exceptions to Notice and Opt Out Requirements

As noted above, section 502(e) contains several exceptions to the requirements that otherwise would apply to the disclosures of nonpublic personal information to nonaffiliated third parties. Proposed § 313.11 set out those exceptions for disclosures that are not made in connection with the administration, processing, servicing, and sale of a consumer's account and made stylistic changes to the statutory language intended to clarify the exceptions. The proposal also provided an example of the consent exception in the context of a financial institution that has received an application from a consumer for a mortgage loan informing a nonaffiliated insurance company that the consumer has applied for a loan. The Commission invited comment on whether safeguards should be added to the exception for consent in order to minimize the potential for consumer confusion.

Several commenters responded to the request for comment on whether the consent exception should include safeguards, such as a requirement that the consent be written, be indicated by a signature on a separate line, or automatically terminate after a certain period of time. Of these, some favored the additional safeguards discussed in the proposal, while others maintained that such precautions are unnecessary. Several suggested that the consent exception include a provision noting that participation in a program where a consumer receives ''bundled'' products and services (such as would be the case, for instance, in an affinity program) necessarily implies consent to the disclosure of information between the entities that provide the bundled products or services. Others suggested that certain terms and conditions be imposed on any consent agreement, such as a time by which the financial institution must stop disclosing nonpublic personal information once a consent is revoked.

The Commission has declined to elaborate on the requirements for obtaining consent or the consumer safeguards that should be in place when a consumer consents. The resolution of this issue is appropriately left to the particular circumstances of a given transaction. Any financial institution that obtains the consent of a consumer to disclose nonpublic personal information should take steps to ensure that the limits of the consent are well understood by both the financial institution and the consumer. If misunderstandings arise, consumers may have means of redress, such as in situations when a financial institution obtains consent through a deceptive or fraudulent practice. Moreover, a consumer may always revoke his or her consent. In light of the safeguards already in place, the Commission has decided not to add safeguards to the consent exception.

Many commenters offered specific suggestions for additional exceptions or amendments to the proposed exceptions. In many cases, the suggestions are accommodated elsewhere in the regulation (such as is the case, for instance, for exceptions to permit (a) verification of available funds or (b) disclosures to or by appraisers, flood insurers, attorneys, insurance agents, or mortgage brokers to effect a transaction). In other cases, the suggestions are inconsistent with the statute (as is the case, for instance, with one commenter's suggestion that the Commission completely exempt a financial institution from all of the statute's requirements if the institution makes no disclosures other than what is permitted by section 502(e)). Accordingly, the Commission has retained, in § 313.15, the statement of the exceptions as proposed and invites interested parties to seek clarifications as necessary in their particular circumstance. See 16 CFR pt. 1.

Section 313.16 Protection of the Fair Credit Reporting Act

Section 506 of the G-L-B Act makes several amendments to the FCRA to vest rulemaking authority in various agencies and to restore the Agencies' regular examination authority. Paragraph (c) of section 506 states that, except for the amendments noted regarding rulemaking authority, nothing in Title V of the G-L-B Act is to be construed to modify, limit, or supersede the operation of the FCRA, and no inference is to be drawn on the basis of the provisions of Title V whether information is transaction or experience information under section 603 of the FCRA. Proposed § 313.14 implemented section 506(c) of the G-L-B Act by restating the statute, making only minor stylistic changes intended to make the rule clearer.

Comments about this provision focused mainly on whether the Commission, by requiring annual notice of a consumer's right to opt out under the FCRA, was modifying, limiting, or superseding the operation of the FCRA. For the reasons explained in the discussion of § 313.6, above, the annual disclosure mandated by the G-L-B Act does not affect the obligations imposed by the FCRA.

Other commenters suggested that this section protects the ability of consumer reporting agencies to disclose credit header information to unaffiliated third parties. As discussed in § 313.11 above, the Commission disagrees with this position. Finally, at least one commenter requested that the Commission specifically reference provisions of the Fair Credit Reporting Act that are not modified, limited, or superceded by the G-L-B Act. Such an approach is not necessary to implement section 506 of the Act and, therefore, the final rule adopts in § 313.16 the text set out in § 313.14 of the proposal.

Section 313.17 Relation to State Laws

Section 507 of the G-L-B Act states, in essence, that Title V does not preempt any State law that provides greater protections than are provided by Title V. Determinations of whether a State law or Title V provides greater protections are to be made by the Commission after consultation with the agency that regulates either the party filing a complaint or the financial institution about which the complaint was filed, and may be initiated by any interested party or on the Commission's own motion. The Act does not require such determinations for consistent state laws. Some commenters suggested that the Commission lacks the authority to consider preemption issues with respect to the rule, but only with respect to the Act. The Commission disagrees with the analysis. Any determination of whether a state law provides greater protection than the Act will necessarily require consideration of the rules that implement the Act.

Comments on this section ranged from those who suggested that federal law should preempt state law in every case where there is a conflict to those who encouraged the Commission to support the rights of states to enact greater protections. Some requested clarification of whether a particular state law would be considered more restrictive, while others suggested that the Commission establish in the final rule a choice of law principle for financial institutions operating in more than one state. These and other suggestions exceed the scope of this rulemaking and are better addressed, to the extent practicable, in the context of a preemption determination. Accordingly, the Commission has adopted in § 313.17 the text set out in proposed § 313.15.

Section 313.18 Effective Date; Transition Rule

Section 510 of the G-L-B Act states that, as a general rule, the relevant provisions of Title V take effect 6 months after the date on which rules are required to be prescribed, *i.e.,* November 13, 2000. However, section 510(1) authorizes the Commission to prescribe a later date in the rule enacted pursuant to section 504. The proposed rule sought comment on the effective date prescribed by the statute. It also would have required that financial institutions provide initial notices, within 30 days of the effective date of the final rule, to people who were customers as of the effective date. The preamble to the proposed rule noted that a financial institution would have to provide opt out notices before the rule's effective date if the institution wanted to continue sharing nonpublic personal information with nonaffiliated third parties without interruption.

The overwhelming majority of commenters addressing this provision requested additional time to comply with the final rule. Commenters stated that six months would not be sufficient to take the steps needed to comply with the regulation, including preparing new disclosure forms, developing software needed to track opt outs, training employees, creating management oversight systems, and undergoing internal examination and auditing to ensure compliance. Several commenters suggested that it would be less effective and potentially more confusing for consumers to receive several notices all around the end of the year 2000 than it would be for the notices to be delivered during a rolling phase-in. Others noted that the proposed effective date would place a severe strain on financial institutions at a time when other year-end notices need to be prepared and delivered. Several commenters noted that financial institutions have not budgeted for the expenses in the current year that likely will be incurred. They also noted that the disclosures regarding the standards to be followed to protect customers' records have not been proposed for comment, thereby making it impossible for financial institutions to know how to prepare at least that part of the initial privacy notices. Requests for extensions of the effective date typically ranged from 12 months to 24 months from publication of the rule.

Many commenters also stated that a 30-day phase-in for initial notices to existing customers is not feasible, given the large number of notices, the short period of time allowed, and the competing demands on financial institutions at the time when the initial notices must be sent. A few suggested that the rule require initial notices to be sent only to people who establish customer relationships after the effective date of the rule and allow a financial institution to send annual notices to existing customers at some point during the next 12 months and annually thereafter.

The Commission agrees that six months may be insufficient in certain instances for a financial institution to ensure that its forms, systems, and procedures comply with the rule. In order to accommodate situations requiring additional time, the Commission has retained the effective date of November 13, but, consistent with its authority under section 510(1) of the G-L-B Act to extend the effective date, the Commission will give financial institutions until July 1, 2001 to be in full compliance with the regulation. Financial institutions are expected, however, to begin compliance efforts promptly, to use the period prior to June 30, 2001 to implement and test their systems, and to be in full compliance by July 1, 2001. Because financial institutions will have slightly over 13 months in which to comply with the rule, there no longer is any need for a separate phase-in for providing initial notices. Thus, a financial institution will need to deliver all required opt out notices and initial notices before July 1, 2001. This extension represents a fair balance between those seeking prompt implementation of the protections afforded by the statute and those concerned about the reliability of the systems that are put in place.

Financial institutions are encouraged to provide disclosures as soon as practicable. Institutions that do not disclose nonpublic personal information to third parties have fewer burdens under the rule (both in terms of notice requirements and opt out mechanism) and should therefore be able to provide privacy notices to their consumers more expeditiously. Depending on the readiness of an institution to process opt out elections, institutions might wish to consider including the privacy and opt out notices in the same mailing as is used to provide tax information to consumers in the first quarter of 2001 so that consumers are less likely to overlook the notices.

The Commission has concluded that the extension of the date by which financial institutions must be in full compliance provides much of the relief sought by those who suggested that initial notices should not be required for existing customers. By allowing financial institutions to deliver notices over a significantly longer period of time than was proposed, the concentrated burden that would have been imposed by the proposed rule is avoided. Accordingly, the Commission

has decided not to adopt the suggestion that initial notices be required only for new customers after the effective date of the rule. Initial notices need not be given to customers whose relationships have terminated prior to the date by which institutions must be in compliance with the rule. Thus, if an account is inactive according to a financial institution's policies before July 1, 2001, then no initial notice would be required in connection with that account. However, because these former customers would remain consumers, a financial institution would have to provide a privacy and opt out notice to them if the financial institution intended to disclose their nonpublic personal information to nonaffiliated third parties beyond the exceptions in §§ 313.14 and 313.15.

The Commission notes that full compliance with the rule's restrictions on disclosures is required on July 1, 2001. To be in full compliance, institutions must have provided their existing customers with both a privacy notice and a reasonable amount of time to opt out prior to that date. If these have not been provided, the disclosure restrictions will apply. This means that a financial institution would have to cease sharing customers' nonpublic personal information with nonaffiliated third parties on that date, unless it may share the information pursuant to an exception under §§ 313.14 or 313.15. However, financial institutions that both provide the privacy notice and allow a reasonable period of time to opt out before July 1, 2001 may continue to share nonpublic personal information after that date about customers who do not opt out.

The Commission's final rule provides for an exception to the effective date to take into consideration the Board's authority to add activities that are permissible for financial holding companies to engage in. The Board's addition of permissible activities (''subsequent permissible activities'') will cause some entities that are not now financial institutions to come within the definition at a later date. The exception provides that the rule is not effective as to any entity engaging in subsequent permissible activities until the Commission so determines.

The Board has the authority to allow financial holding companies to engage in activities that are financial in nature, activities that are incidental to financial activities, and activities that are complementary to financial activities. If the Board, therefore, issues an order or regulation identifying the activity that the financial holding company may engage in without characterizing that activity, the Commission will have to determine whether any entities engaging in such activity should be covered by the privacy provisions of the G-L-B Act and, if so, to what extent. The Commission intends to publish for notice and comment its proposals with respect to entities engaging in subsequent permissible activities.

Appendix A—Sample Clauses

In order to provide additional guidance to financial institutions concerning the level of detail the Commission believe is appropriate under the statute, the Commission has set forth a variety of sample clauses for financial institutions to consider. The Commission urges financial institutions to carefully review whether these clauses accurately reflect a given institution's policies and practices before using the clauses. Financial institutions are free to use different language and to include as much additional detail as they think is appropriate in their notices.

Derivation Chart

Below is a chart showing the derivation of the sections in the final privacy rule from the proposal. Only changes are noted.

Proposal	Content of provision	Final rule
4(d)	How to provide initial notice	9(a)
N/A	New product for existing customer	4(d)
4(d)(3)	Oral delivery (privacy notice)	9(d)
4(d)(4)	Retainable notice	9(e)
N/A	Joint relationships (privacy notice)	4(f)
5(b)	How to provide annual notice	9(a) and (c)
5(c)	Terminated customer relationships	5(b)
N/A	Delivering short-form initial notices	6(d)(3)
7	Main operative provision	10
8(a)	Opt out methods; opt out notice content	7(a)
8(b)(1)	How to deliver opt out notices	9(a)
8(b)(2)	Oral delivery (opt out notice)	9(d)
8(b)(3)	Same form as initial notice	7(b)
8(b)(4)	Initial notice must accompany opt out notice	7(c)
N/A	Joint relationships (opt out notice)	7(d)
8(d)	Time to comply with opt out; continuing right to opt out	7(e) and (f)
8(e)	Duration of opt out	7(g)
8(c)(1)	Revised notices	8(a)
8(c)(2)	How to deliver revised notice	8(c)
8(c)(3)	Examples of when revised notice is required	8(b)
9	Exception for service providers and joint marketers	13
10	Exceptions for processing and servicing transactions	14
11	Other exceptions	15
12	Redisclosure and reuse	11
13	Sharing account number information	12
14	FCRA	16
15	State law	17
16	Effective date	18

Section D. Guidance for Certain Institutions

To minimize the burden and costs to a financial institution (''you'') and generally clarify the operation of the final rule, the Agencies have included this guidance that you may use in conjunction with the sample clauses in Appendix A. This guidance specifically applies to you if you:

(1) do not have any affiliates;

(2) only disclose nonpublic personal information to nonaffiliated third

parties in accordance with an exception under §§ 313.14 or 313.15, such as in connection with servicing or processing a financial product or service that a consumer requests or authorizes ; and

(3) do not reserve the right to disclose nonpublic personal information to nonaffiliated third parties, except under §§ 313.14 and 313.15. [39]

In addition, if you disclose nonpublic personal information in accordance with the exception in § 313.13 for service providers and joint marketers, you also must include an accurate description of that information, as illustrated by the sample clause in section *(K)* below.

In general, if you disclose nonpublic personal information to nonaffiliated third parties only as authorized under an exception, then your only responsibilities under the regulation are to provide initial and annual notices to each of your customers. You do not need to provide an opt out notice or opt out rights to your customers.

A. Initial notice to customers. You must provide an initial notice to each of your customers. A customer is a natural person who has a continuing relationship with you, as described in § 313.4(c). For instance, a ''pay day'' lender who extends a loan to an individual has a customer relationship with that individual. By contrast, if the ''pay day'' lender only cashes a check for that individual, there is no customer relationship; even if that individual repeatedly cashes checks with the same pay-day lender, she remains only the lender's consumer. In other words, you must provide initial and annual notices to each of your customers, but not to others.

B. Time to provide initial notice. You must provide an initial privacy notice to each of your customers not later than when you establish a customer relationship (§ 313.4(a)(1)). For instance, you must provide a privacy notice to an individual not later than when that individual executes the contract to open a checking account. Thus, you can provide the notice to a checking account customer together with the account agreement and signature card.

Similarly, in the case of extending a mortgage loan, you must provide a privacy notice to an individual not later than when you and the individual enter into an agreement that you will serve as the mortgage lender. For example, you can provide the notice to an individual together with the documents (or other forms) that constitute the contract to extend the loan. You may always deliver your privacy notices earlier than required.

If one of your existing customers obtains a new financial product or service from you, then you need not provide another initial notice to that customer (§ 313.4(d)) if that earlier notice covered the subsequent product.

For instance, if Alison Individual enters Lender's offices for the first time on July 2, 2001 to obtain a mortgage, then Lender complies with § 313.4(a)(1) of the rule if it provides an initial notice to Alison with the mortgage agreement. When Alison obtains her mortgage, she becomes a customer of Lender. Alison makes regular payments to Lender on her mortgage and, two years later, returns to Lender to obtain a credit card. If the initial notice that Lender provided to Alison is accurate with respect to the terms of that credit card, then Lender need not provide another initial notice to her when she obtains the credit card because Lender has already provided a notice to Alison that covers that relationship.

C. Method of providing the initial notice. You must provide your initial notice so that each customer can reasonably be expected to receive actual notice of it, in writing (§ 313.9(a)). For example, you may provide the initial notice by mailing a printed copy of it together with a loan contract. Similarly, you may provide the initial notice by hand-delivering a printed copy of it to the customer together with a deposit account agreement.

D. Compliance with initial notice requirement for existing customers by effective date. You must provide an initial notice to each of your current customers not later than July 1, 2001 (§ 313.18(b)). You may do so by mailing a printed copy of the notice to the customer's last known address.

E. Annual notice. During the continuation of the customer relationship, you must provide an annual notice to the customer, as described in § 313.5(a). You must provide an annual notice to each customer at least once in any period of 12 consecutive months during which the customer relationship exists. You may define the 12-consecutive-month period, but must consistently apply that period to the customer. You may define the 12-consecutive-month period as a calendar year and provide the annual notice to the customer once in each calendar year following the calendar year in which you provided the initial notice.

For example, assume that Lender defines the 12-consecutive-month period as a calendar year and provides annual notices to all of its customers on October 1 of each year. If Alison Individual obtained her mortgage with Lender on July 2, 2001, thereby becoming a customer, then Lender must provide an initial notice to Alison together with the mortgage agreement or earlier. Lender must provide an annual notice to Alison by December 31, 2002. If Lender provides an annual notice to Alison on October 1, 2002, as it does for other customers, then it must provide the next annual notice to Alison not later than October 1, 2003.

F. Method of providing the annual notice. Like the initial notice, you must provide the annual notice so that each customer can reasonably be expected to receive actual notice of it, in writing (§ 313.9(a)). You may do so by mailing a printed copy of the notice to the customer's last known address.

G. Joint accounts. If two or more customers jointly obtain a financial product or service, then you may provide one initial notice to those customers jointly. Similarly, you may provide one annual notice to those customers jointly (§ 313.4(f)).

H. Information described in the initial and annual notices. The initial and annual notices must include an accurate description of the following four items of information:

(a) The categories of nonpublic personal information that you collect (§ 313.6(a)(1));

(b) The fact that you do not disclose nonpublic personal information about your current customers to affiliates or nonaffiliated third parties, except as authorized by §§ 313.14 and 313.15 (§ 313.6(a)(2)–(3), (9)). When describing the categories with respect to those parties, you are required to state only that you make disclosures to other nonaffiliated third parties as permitted by law (§ 313.6(b));

(c) The categories of nonpublic personal information about your former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your former customers (§ 313.6(a)(4));

(d) Your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information (§ 313.6(a)(8)).

For each of these four items of information above, you may use a sample clause from Appendix A. The Agencies emphasize that you may use a sample clause only if that clause

[39] If you disclose or reserve the right to disclose nonpublic personal information to a nonaffiliated third party under other circumstances, you must comply with other provisions in the rule, notably §§ 313.7, 313.8, and 313.13, if applicable. If you disclose or reserve the right to disclose nonpublic personal information to an affiliate you must comply with other provisions in the rule, notably § 313.6(a)(7), as applicable.

accurately describes your actual policies and practices.

I. Example of notice. A financial institution (''Lender'') that (i) does not have any affiliates and (ii) only discloses nonpublic personal information to nonaffiliated third parties as authorized under §§ 313.14 and 313.15, may comply with the requirements of § 313.6 of the rule by using the following notice, if applicable.

Lender collects nonpublic personal information about you from the following sources:

- *Information we receive from you on applications or other forms;*
- *Information about your transactions with us or others; and*
- *Information we receive from a consumer reporting agency.*[40]

We do not disclose any nonpublic personal information about you to anyone, except as permitted by law.

If you decide to pay off your loan(s), we will adhere to the privacy policies and practices as described in this notice.

Lender restricts access to your personal and account information to those employees who need to know that information to provide products or services to you. Lender maintains physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

J. Initial and annual notices must be clear and conspicuous. The Commission emphasizes that you must ensure that both the initial and annual notices are clear and conspicuous, as defined in § 313.3(b).

K. Example of notice for disclosure to service providers and joint marketers. If you disclose nonpublic personal information in accordance with the exception in § 313.13, for service providers and joint marketers, you also must include an accurate description of that information. You may comply with the requirements of § 313.13 of the rule by including the following sample clause, if applicable, in the example of notice described in section (*I*) above:

We may disclose all of the information we collect, as described [describe location in the notice, such as ''above'' or ''below'], to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

[40] You only need to describe those general categories that apply to your policies and practices. Accordingly, if you do not collect information from ''a consumer reporting agency,'' for instance, then you need not describe that category in your notices.

Section E. Final Regulatory Flexibility Analysis

The Regulatory Flexibility Act (5 U.S.C. 601–612) (''RFA'') requires, subject to certain exceptions, that federal agencies prepare an initial regulatory flexibility analysis (''IRFA'') with a proposed Rule and a final regulatory flexibility analysis (''FRFA'') with a final Rule, unless the agency certifies that the Rule will not have a significant economic impact on a substantial number of small entities. At the time the proposed Rule was issued, the Commission believed that the G-L-B Act's requirements accounted for most, if not all, of the economic impact of the Rule, but decided to publish the IRFA to ensure that in developing the final Rule it adequately considered the impact on small businesses. After reviewing the comments submitted in response to the proposed Rule, the Commission continues to believe that the burden imposed on small institutions stems primarily from the statute and that certification would be proper. However, in order to assist those entities with comprehending and complying with the final Rule, the Commission has determined that it is appropriate to publish a FRFA analyzing the Rule as a whole and highlighting provisions that will particularly accommodate the needs of small businesses.

This FRFA incorporates the Commissions's initial findings, as set forth in the IRFA; addresses the comments submitted in response to the IRFA; and describes the steps the Commission has taken in the final Rule to minimize the impact on small entities, consistent with the objectives of the G-L-B Act. The Commission is publishing with this part a guide for entities that do not share any nonpublic personal information, a disproportionate number of which are likely to be small businesses. (See Supplementary Information, Section C.) Also, in accordance with Section 212 of the Small Business Regulatory Enforcement Fairness Act of 1996 (Public Law 104–121), the Commission will in the near future issue a compliance guide to assist small entities in complying with this rule.

Succinct Statement of the Need for, Objectives of, and Legal Basis for the Rule

The final Rule implements the provisions of Title V, Subtitle A of the G-L-B Act, which addresses consumer privacy. In general, these statutory provisions require financial institutions to provide notice to consumers about the institution's privacy policies and practices, describe the conditions under which financial institutions may disclose nonpublic personal information about consumers to nonaffiliated third parties, and permit consumers to prevent institutions from sharing nonpublic personal information about them with certain non-affiliated third parties by ''opting out'' of that disclosure.

Section 504 of the G-L-B Act requires the Commission to prescribe ''such regulations as may be necessary'' to carry out the purposes of Title V, Subtitle A. In the absence of these regulations, the substantive burdens imposed by the Act (*e.g.,* the notice, information-sharing restrictions, and opt-out requirements) would have become effective and binding upon financial institutions within one year of the enactment of the law. The Commission believes that the final Rule gives the private sector greater certainty and flexibility with respect to compliance with the statute, as well as clearer guidance as to how the Commission will enforce it.

Description and Estimate of the Number of Small Entities to Which the Proposed Rule Will Apply

Determining a precise estimate of the number of small entities that are financial institutions within the meaning of the proposed Rule is not readily feasible. The definition of ''financial institution'' includes any institution the business of which is engaging in a financial activity, as described in section 4(k) of the Bank Holding Company Act, which incorporates by reference the activities listed in 12 CFR 225.28 and 12 CFR 211.5(d). These include lenders, loan brokers and servicers, collection agencies, financial advisors, tax preparers, real estate settlement services, property appraisers, and others. The G-L-B Act does not identify for purposes of the Commission's jurisdiction any specific category of financial institution; section 505(a)(7) vests the Commission with enforcement authority with respect to ''any other financial institution or other person that is not subject to the jurisdiction of any [other] agency or authority [charged with enforcing the statute].'' Jurisdiction is assigned to other agencies with respect to banks, bank holding companies, and their subsidiaries and affiliates; savings associations, federal credit unions, and their subsidiaries; securities brokers and dealers; investment advisers and investment companies; and insurers.

Although the Commission requested comment on these issues, it did not receive a response sufficient to provide a basis for determining the number of small entities subject to the final Rule. In the absence of such information, there is no way to estimate precisely the number of affected entities that share nonpublic personal information with nonaffiliated third parties or that establish customer relationships with consumers and therefore assume greater disclosure obligations.

Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements

The Commission incorporates by reference its description of the projected reporting, recordkeeping, and other compliance requirements of the Rule, as set forth in the IRFA. The Commission has not received any comments that necessitate modification of its previous description of projected compliance requirements. Based on the information the Commission submitted to the Office of Management and Budget, which included an estimated average annual burden over the three-year period of clearance of 4.03 million hours and $87.3 million, OMB has approved the final Rule for the related purposes of the Paperwork Reduction Act. (See section F, infra.)

Among the principal obligations that Title V, Subtitle A of the G-L-B Act, as executed by the final Rule, imposes upon financial institutions is the preparation of notices explaining their privacy policies and practices. Institutions are required to provide those notices to consumers as specified in the Rule, and institutions that disclose nonpublic personal information about their consumers to nonaffiliated third parties will be required to provide opt out notices, as well as a reasonable opportunity to opt out of certain disclosures, to their consumers. These institutions will have to develop systems for keeping track of consumers' opt out directions. Some institutions, particularly those that disclose nonpublic information about consumers to nonaffiliated third parties, will likely need the advice of legal counsel to ensure that they comply with the Rule and may also require computer programming changes and additional staff training.

A detailed, section-by-section analysis of the final Rule is set forth above in section B. of the Supplementary Information part of this notice.

Summary of Significant Issues Raised by Public Comments and Description of Steps the Commission Has Taken To Minimize the Significant Economic Impact on Small Entities

The Commission has sought to minimize the burden on all businesses, including small entities, in promulgating this final rule. Although one method of accomplishing this objective would be to adopt a specific exemption for small entities, the G-L-B Act does not authorize the Commission to create exemptions based on an institution's size. Further, the Commission believes that different compliance standards would be inconsistent with the purpose of Title V, which is to offer all consumers some measure of control over the dissemination of the nonpublic personal information that they provide to financial institutions, regardless of the institution's size. As section 501(a) of the Act declares, ''[i]t is the policy of the Congress that *each* financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.'' (Emphasis added).

Notwithstanding its limited authority to accommodate the specific needs of smaller institutions, the Commission has requested and analyzed throughout this rulemaking process information regarding the economic impact of the G-L-B Act's requirements for all financial institutions, including small entities. The proposed rule and the IRFA included a number of questions for public comment regarding the costs associated with complying with the Rule and the impact on small entities. Although the Commission received few comments that specifically addressed the regulatory flexibility analysis, it carefully considered comments concerning the substantive provisions of the Rule.[41] The discussion below reviews some of those key recommendations and corresponding changes adopted in the final Rule that accommodate those suggestions. Many of the steps taken by the Commission will benefit all institutions, regardless of size, while others will especially reduce the regulatory burden for small entities. For a more complete discussion of these changes, see the section-by-section analysis under section C of the Supplementary Information part of this notice.

Effective Date

Subject to section 510 of the G-L-B Act, the relevant provisions of Title V take effect on November 13, 2000. However, section 510(1) authorizes the Commission to prescribe a later date in the regulations enacted pursuant to section 504. The proposed Rule sought comment on the effective date prescribed by the statute. The overwhelming majority of commenters requested additional time to comply with the final rule. Several commenters noted that financial institutions may encounter difficulty managing the expenses and resources required to comply with the final rule as the institution's budget for the current year was established prior to the issuance of the proposed regulation. This may be especially true for small institutions that face already tight budgetary constraints due to heightened competition. In response to these concerns, the Commission has retained the effective date of November 13, 2000 but, consistent with its authority under section 510(1) of the statute, will give financial institutions until July 1, 2001 to be in full compliance with the final Rule. This additional time should reduce compliance costs for institutions by allowing additional time to budget for any necessary expenses and to implement all necessary operational changes required to comply with this Rule.

Examples

Throughout the final Rule, the Commission has included examples of conduct that illustrate ways to comply with particular provisions. As the section-by-section analysis above and the Rule itself explain, these examples are not exclusive, but they should lessen for institutions the burdens imposed by the Rule by clarifying that compliance with an applicable example constitutes compliance with the applicable provision.

Definition of Nonpublic Personal Information

In the proposed rule, the Commission provided two alternatives for defining nonpublic personal information. The

[41] Even if the Commission had the authority to craft exceptions strictly based on the size of institutions, the comments received did not provide the amount, specificity, or consistency of information required to make such targeted policy determinations. For example, the Commission received one comment from a regional department store retailer with an estimated annual volume of $700 million in 1999. This small retail chain stated that approximate mailing costs associated with issuing privacy notices would be $400,000–$500,000, or 4%–5% of its net income. Another commenter estimated that total compliance costs would total $97,400 for an institution with assets of approximately $100 million. Based on these widely disparate projections and scant statistics, an exception applicable to all ''small entities'' would be impracticable and inappropriate.

first, (Alternative A) deemed information as publicly available only if a financial institution *actually obtained* the information from a public source, whereas the second (Alternative B) treated information as publicly available if a financial institution *could* obtain it from such a source. A vast majority of commenters favored Alternative B as significantly less burdensome than Alternative A. In response to these comments, the final Rule adopts a modified version of Alternative B, which is more fully explained in the section-by-section analysis.

Content of Notices

Many commenters interpreted the proposed Rule as mandating lengthy, confusing privacy notices that would offer little benefit to consumers, and asked for clarification with respect to the content of those disclosures. Although the Commission believes that the notice obligations are not unduly burdensome, in the final Rule it has taken a number of steps to clarify the requirements imposed by the G-L-B Act. The final Rule substantially revises the examples of disclosures that would satisfy the Rule, includes sample clauses that might be used, and adds a new provision for ''short-form'' privacy notices to a consumer that does not become a customer, provided the institution gives the consumer an opt out notice and a reasonably convenient method of obtaining a copy of the full privacy notice. It also retains the simplified notice provision for institutions that do not share nonpublic personal information with nonaffiliated third parties, except pursuant to the exceptions set forth in §§ 313.14 and 313.15 of this part. These measures may be particularly helpful to smaller institutions who do not disclose nonpublic personal information except under those and other exceptions in the final Rule.

In addition, the Commission has included with the final Rule sample disclosures that institutions may use to draft their privacy and opt out notices required by this part. As discussed in the section-by-section analysis above, these clauses are provided to convey to institutions the requisite level of detail that these notices must contain. Institutions can also consult the Guide for Certain Financial Institutions (''Guide''). The Guide generally clarifies the operation of the final Rule. It also provides an example of a notice for institutions, including small entities, that only share nonpublic personal information with nonaffiliated third parties pursuant to the exceptions provided in §§ 313.14 and 313.15. The Guide may be used in conjunction with the sample clauses contained in Appendix A. Like the examples discussed above, the sample disclosures and the Guide are intended to minimize the burden of complying with the final Rule, by reducing, among other costs, the need for legal advice.

Joint Account Holders

Another frequent comment addressed the provision of notice to and effect of opt outs exercised by joint account holders. As the section-by-section analysis describes, the final Rule clarifies that institutions may provide a single notice to joint account holders (unless otherwise requested), with the understanding that a decision to opt out made by one of the joint account holders will, absent a provision to the contrary in the opt out notice, be effective with respect to each of the account holders. By reducing the number of notices that institutions are required to provide, this flexibility will particularly benefit those institutions, including small entities, that do not share nonpublic personal information with nonaffiliated third parties, except pursuant to an exception.

New Notices Not Required for Each New Financial Product or Service

Some commenters expressed concern that the proposed rule may require a new initial notice each time a consumer obtains a new financial product or service. This would be especially burdensome for an institution that adopts a universal privacy policy that covers multiple products and services. To address these concerns and minimize economic burden, the final Rule was clarified to instruct institutions that a new initial notice is not required if the institution has given the customer the institution's initial notice, and that notice remains accurate with respect to the new product or service.

Section F. Paperwork Reduction Act

Pursuant to the Paperwork Reduction Act, as amended, 44 U.S.C. 3501 *et seq.*, the Commission submitted the proposed Rule to the Office of Management and Budget (OMB) for review. The OMB has approved the Rule's information collection requirements.[42] A **Federal Register** notice with a 30-day comment period of soliciting comments on this collection of information was published on March 1, 2000 (65 FR 11174). The Commission did not receive any comments that necessitated modifying its original burden estimates for the Rule's notice requirements.

Section G. Final Rule

List of Subjects in 16 CFR Part 313

Consumer protection, Credit, Data protection, Privacy, Trade practices.

Accordingly, the Commission amends 16 CFR Ch. I, Subchapter C, by adding a new Part 313 to read as follows:

PART 313—PRIVACY OF CONSUMER FINANCIAL INFORMATION

Sec.

Authority: 15 U.S.C. 6801 *et seq.*

§ 313.1 Purpose and scope.

(a) *Purpose.* This part governs the treatment of nonpublic personal information about consumers by the financial institutions listed in paragraph (b) of this section. This part:

(1) Requires a financial institution in specified circumstances to provide notice to customers about its privacy policies and practices;

(2) Describes the conditions under which a financial institution may

[42] The assigned OMB clearance number is 3084–0121.

disclose nonpublic personal information about consumers to nonaffiliated third parties; and

(3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by ''opting out'' of that disclosure, subject to the exceptions in §§ 313.13, 313.14, and 313.15.

(b) *Scope.* This part applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family or household purposes from the institutions listed below. This part does not apply to information about companies or about individuals who obtain financial products or services for business, commercial, or agricultural purposes. This part applies to those ''financial institutions'' and ''other persons'' over which the Federal Trade Commission (''Commission'') has enforcement authority pursuant to Section 505(a)(7) of the Gramm-Leach-Bliley Act. An entity is a ''financial institution'' if its business is engaging in a financial activity as described in Section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k), which incorporates by reference activities enumerated by the Federal Reserve Board in 12 CFR 211.5(d) and 12 CFR 225.28. The ''financial institutions'' subject to the Commission's enforcement authority are those that are not otherwise subject to the enforcement authority of another regulator under Section 505 of the Gramm-Leach-Bliley Act. More specifically, those entities include, but are not limited to, mortgage lenders, ''pay day'' lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors that are not required to register with the Securities and Exchange Commission. They are referred to in this part as ''You.'' The ''other persons'' to whom this part applies are third parties that are not financial institutions, but that receive nonpublic personal information from financial institutions with whom they are not affiliated. Nothing in this part modifies, limits, or supersedes the standards governing individually identifiable health information promulgated by the Secretary of Health and Human Services under the authority of sections 262 and 264 of the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d–1320d–8. Any institution of higher education that complies with the Federal Educational Rights and Privacy Act (''FERPA''), 20 U.S.C. 1232g, and its implementing regulations, 34 CFR part 99, and that is also a financial institution subject to the requirements of this part, shall be deemed to be in compliance with this part if it is in compliance with FERPA.

§ 313.2 Rule of construction.

The examples in this part and the sample clauses in Appendix A of this part are not exclusive. Compliance with an example or use of a sample clause, to the extent applicable, constitutes compliance with this part. For non-federally insured credit unions, compliance with an example or use of a sample clause contained in 12 CFR part 716, to the extent applicable, constitutes compliance with this part. For intrastate securities broker-dealers and investment advisors not registered with the Securities and Exchange Commission, compliance with an example or use of a sample clause contained in 17 CFR part 248, to the extent applicable, constitutes compliance with this part.

§ 313.3 Definitions.

As used in this part, unless the context requires otherwise:

(a) *Affiliate* means any company that controls, is controlled by, or is under common control with another company.

(b)(1) *Clear and conspicuous* means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) *Examples*—(i) *Reasonably understandable.* You make your notice reasonably understandable if you:

(A) Present the information in the notice in clear, concise sentences, paragraphs, and sections;

(B) Use short explanatory sentences or bullet lists whenever possible;

(C) Use definite, concrete, everyday words and active voice whenever possible;

(D) Avoid multiple negatives;

(E) Avoid legal and highly technical business terminology whenever possible; and

(F) Avoid explanations that are imprecise and readily subject to different interpretations.

(ii) *Designed to call attention.* You design your notice to call attention to the nature and significance of the information in it if you:

(A) Use a plain-language heading to call attention to the notice;

(B) Use a typeface and type size that are easy to read;

(C) Provide wide margins and ample line spacing;

(D) Use boldface or italics for key words; and

(E) In a form that combines your notice with other information, use distinctive type size, style, and graphic devices, such as shading or sidebars, when you combine your notice with other information.

(iii) *Notices on web sites.* If you provide a notice on a web page, you design your notice to call attention to the nature and significance of the information in it if you use text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice, and you either:

(A) Place the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(B) Place a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

(c) *Collect* means to obtain information that you organize or can retrieve by the name of an individual or by identifying number, symbol, or other identifying particular assigned to the individual, irrespective of the source of the underlying information.

(d) *Company* means any corporation, limited liability company, business trust, general or limited partnership, association, or similar organization.

(e)(1) *Consumer* means an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.

(2) *Examples*—(i) An individual who applies to you for credit for personal, family, or household purposes is a consumer of a financial service, regardless of whether the credit is extended.

(ii) An individual who provides nonpublic personal information to you in order to obtain a determination about whether he or she may qualify for a loan to be used primarily for personal, family, or household purposes is a consumer of a financial service, regardless of whether the loan is extended.

(iii) An individual who provides nonpublic personal information to you in connection with obtaining or seeking to obtain financial, investment, or

economic advisory services is a consumer, regardless of whether you establish a continuing advisory relationship.

(iv) If you hold ownership or servicing rights to an individual's loan that is used primarily for personal, family, or household purposes, the individual is your consumer, even if you hold those rights in conjunction with one or more other institutions. (The individual is also a consumer with respect to the other financial institutions involved.) An individual who has a loan in which you have ownership or servicing rights is your consumer, even if you, or another institution with those rights, hire an agent to collect on the loan.

(v) An individual who is a consumer of another financial institution is not your consumer solely because you act as agent for, or provide processing or other services to, that financial institution.

(vi) An individual is not your consumer solely because he or she has designated you as trustee for a trust.

(vii) An individual is not your consumer solely because he or she is a beneficiary of a trust for which you are a trustee.

(viii) An individual is not your consumer solely because he or she is a participant or a beneficiary of an employee benefit plan that you sponsor or for which you act as a trustee or fiduciary.

(f) *Consumer reporting agency* has the same meaning as in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

(g) *Control* of a company means:

(1) Ownership, control, or power to vote 25 percent or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;

(2) Control in any manner over the election of a majority of the directors, trustees, or general partners (or individuals exercising similar functions) of the company; or

(3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company.

(h) *Customer* means a consumer who has a customer relationship with you.

(i)(1) *Customer relationship* means a continuing relationship between a consumer and you under which you provide one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes.

(2) *Examples*—(i) *Continuing relationship.* A consumer has a continuing relationship with you if the consumer:

(A) Has a credit or investment account with you;

(B) Obtains a loan from you;

(C) Purchases an insurance product from you;

(D) Holds an investment product through you, such as when you act as a custodian for securities or for assets in an Individual Retirement Arrangement;

(E) Enters into an agreement or understanding with you whereby you undertake to arrange or broker a home mortgage loan, or credit to purchase a vehicle, for the consumer;

(F) Enters into a lease of personal property on a non-operating basis with you;

(G) Obtains financial, investment, or economic advisory services from you for a fee;

(H) Becomes your client for the purpose of obtaining tax preparation or credit counseling services from you;

(I) Obtains career counseling while seeking employment with a financial institution or the finance, accounting, or audit department of any company (or while employed by such a financial institution or department of any company);

(J) Is obligated on an account that you purchase from another financial institution, regardless of whether the account is in default when purchased, unless you do not locate the consumer or attempt to collect any amount from the consumer on the account;

(K) Obtains real estate settlement services from you; or

(L) Has a loan for which you own the servicing rights.

(ii) *No continuing relationship.* A consumer does not, however, have a continuing relationship with you if:

(A) The consumer obtains a financial product or service from you only in isolated transactions, such as using your ATM to withdraw cash from an account at another financial institution; purchasing a money order from you; cashing a check with you; or making a wire transfer through you;

(B) You sell the consumer's loan and do not retain the rights to service that loan;

(C) You sell the consumer airline tickets, travel insurance, or traveler's checks in isolated transactions;

(D) The consumer obtains one-time personal or real property appraisal services from you; or

(E) The consumer purchases checks for a personal checking account from you.

(j) *Federal functional regulator* means:

(1) The Board of Governors of the Federal Reserve System;

(2) The Office of the Comptroller of the Currency;

(3) The Board of Directors of the Federal Deposit Insurance Corporation;

(4) The Director of the Office of Thrift Supervision;

(5) The National Credit Union Administration Board; and

(6) The Securities and Exchange Commission.

(k)(1) *Financial institution* means any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). An institution that is significantly engaged in financial activities is a financial institution.

(2) *Examples of financial institution.*

(i) A retailer that extends credit by issuing its own credit card directly to consumers is a financial institution because extending credit is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act and issuing that extension of credit through a proprietary credit card demonstrates that a retailer is significantly engaged in extending credit.

(ii) A personal property or real estate appraiser is a financial institution because real and personal property appraisal is a financial activity listed in 12 CFR 225.28(b)(2)(i) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(iii) An automobile dealership that, as a usual part of its business, leases automobiles on a nonoperating basis for longer than 90 days is a financial institution with respect to its leasing business because leasing personal property on a nonoperating basis where the initial term of the lease is at least 90 days is a financial activity listed in 12 CFR 225.28(b)(3) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(iv) A career counselor that specializes in providing career counseling services to individuals currently employed by or recently displaced from a financial organization, individuals who are seeking employment with a financial organization, or individuals who are currently employed by or seeking placement with the finance, accounting or audit departments of any company is a financial institution because such career counseling activities are financial activities listed in 12 CFR 225.28(b)(9)(iii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(v) A business that prints and sells checks for consumers, either as its sole business or as one of its product lines,

is a financial institution because printing and selling checks is a financial activity that is listed in 12 CFR 225.28(b)(10)(ii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(vi) A business that regularly wires money to and from consumers is a financial institution because transferring money is a financial activity referenced in section 4(k)(4)(A) of the Bank Holding Company Act and regularly providing that service demonstrates that the business is significantly engaged in that activity.

(vii) A check cashing business is a financial institution because cashing a check is exchanging money, which is a financial activity listed in section 4(k)(4)(A) of the Bank Holding Company Act.

(viii) An accountant or other tax preparation service that is in the business of completing income tax returns is a financial institution because tax preparation services is a financial activity listed in 12 CFR 225.28(b)(6)(vi) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act.

(ix) A business that operates a travel agency in connection with financial services is a financial institution because operating a travel agency in connection with financial services is a financial activity listed in 12 CFR 211.5(d)(15) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act.

(x) An entity that provides real estate settlement services is a financial institution because providing real estate settlement services is a financial activity listed in 12 CFR 225.28(b)(2)(viii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(xi) A mortgage broker is a financial institution because brokering loans is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(xii) An investment advisory company and a credit counseling service are each financial institutions because providing financial and investment advisory services are financial activities referenced in section 4(k)(4)(C) of the Bank Holding Company Act.

(3) *Financial institution* does not include:

(i) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 *et seq.*);

(ii) The Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 *et seq.*); or

(iii) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as such institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party other than as permitted by §§ 313.14 and 313.15 of this part.

(iv) Entities that engage in financial activities but that are not significantly engaged in those financial activities.

(4) *Examples of entities that are not significantly engaged in financial activities.* (i) A retailer is not a financial institution if its only means of extending credit are occasional ''lay away'' and deferred payment plans or accepting payment by means of credit cards issued by others.

(ii) A retailer is not a financial institution merely because it accepts payment in the form of cash, checks, or credit cards that it did not issue.

(iii) A merchant is not a financial institution merely because it allows an individual to ''run a tab.''

(iv) A grocery store is not a financial institution merely because it allows individuals to whom it sells groceries to cash a check, or write a check for a higher amount than the grocery purchase and obtain cash in return.

(l)(1) *Financial product or service* means any product or service that a financial holding company could offer by engaging in a financial activity under section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) *Financial service* includes your evaluation or brokerage of information that you collect in connection with a request or an application from a consumer for a financial product or service.

(m)(1) *Nonaffiliated third party* means any person except:

(i) Your affiliate; or

(ii) A person employed jointly by you and any company that is not your affiliate (but *nonaffiliated third party* includes the other company that jointly employs the person).

(2) *Nonaffiliated third party* includes any company that is an affiliate by virtue of your or your affiliate's direct or indirect ownership or control of the company in conducting merchant banking or investment banking activities of the type described in section 4(k)(4)(H) or insurance company investment activities of the type described in section 4(k)(4)(I) of the Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

(n)(1) *Nonpublic personal information* means:

(i) Personally identifiable financial information; and

(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

(2) *Nonpublic personal information* does not include:

(i) Publicly available information, except as included on a list described in paragraph (n)(1)(ii) of this section; or

(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.

(3) *Examples of lists*—(i) Nonpublic personal information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information (that is not publicly available), such as account numbers.

(ii) Nonpublic personal information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived, in whole or in part, using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

(o)(1) *Personally identifiable financial information* means any information:

(i) A consumer provides to you to obtain a financial product or service from you;

(ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or

(iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.

(2) *Examples*—(i) *Information included.* Personally identifiable financial information includes:

(A) Information a consumer provides to you on an application to obtain a loan, credit card, or other financial product or service;

(B) Account balance information, payment history, overdraft history, and credit or debit card purchase information;

(C) The fact that an individual is or has been one of your customers or has

obtained a financial product or service from you;

(D) Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;

(E) Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;

(F) Any information you collect through an Internet ''cookie'' (an information collecting device from a web server); and

(G) Information from a consumer report.

(ii) *Information not included.* Personally identifiable financial information does not include:

(A) A list of names and addresses of customers of an entity that is not a financial institution; and

(B) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

(p)(1) *Publicly available information* means any information that you have a reasonable basis to believe is lawfully made available to the general public from:

(i) Federal, State, or local government records;

(ii) Widely distributed media; or

(iii) Disclosures to the general public that are required to be made by Federal, State, or local law.

(2) *Reasonable basis.* You have a reasonable basis to believe that information is lawfully made available to the general public if you have taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that your consumer has not done so.

(3) *Examples*—(i) *Government records.* Publicly available information in government records includes information in government real estate records and security interest filings.

(ii) *Widely distributed media.* Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper, or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(iii) *Reasonable basis*—(A) You have a reasonable basis to believe that mortgage information is lawfully made available to the general public if you have determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(B) You have a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if you have located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

(q) *You* includes each ''financial institution'' (but excludes any ''other person'') over which the Commission has enforcement jurisdiction pursuant to section 505(a)(7) of the Gramm-Leach-Bliley Act.

Subpart A—Privacy and Opt Out Notices

§ 313.4 Initial privacy notice to consumers required.

(a) *Initial notice requirement.* You must provide a clear and conspicuous notice that accurately reflects your privacy policies and practices to:

(1) *Customer.* An individual who becomes your customer, not later than when you establish a customer relationship, except as provided in paragraph (e) of this section; and

(2) *Consumer.* A consumer, before you disclose any nonpublic personal information about the consumer to any nonaffiliated third party, if you make such a disclosure other than as authorized by §§ 313.14 and 313.15.

(b) *When initial notice to a consumer is not required.* You are not required to provide an initial notice to a consumer under paragraph (a) of this section if:

(1) You do not disclose any nonpublic personal information about the consumer to any nonaffiliated third party, other than as authorized by §§ 313.14 and 313.15; and

(2) You do not have a customer relationship with the consumer.

(c) *When you establish a customer relationship*—(1) *General rule.* You establish a customer relationship when you and the consumer enter into a continuing relationship.

(2) *Special rule for loans.* You establish a customer relationship with a consumer when you originate a loan to the consumer for personal, family, or household purposes. If you subsequently transfer the servicing rights to that loan to another financial institution, the customer relationship transfers with the servicing rights.

(3)(i) *Examples of establishing customer relationship.* You establish a customer relationship when the consumer:

(A) Opens a credit card account with you;

(B) Executes the contract to obtain credit from you or purchase insurance from you;

(C) Agrees to obtain financial, economic, or investment advisory services from you for a fee; or

(D) Becomes your client for the purpose of your providing credit counseling or tax preparation services, or to obtain career counseling while seeking employment with a financial institution or the finance, accounting, or audit department of any company (or while employed by such a company or financial institution);

(E) Provides any personally identifiable financial information to you in an effort to obtain a mortgage loan through you;

(F) Executes the lease for personal property with you;

(G) Is an obligor on an account that you purchased from another financial institution and whom you have located and begun attempting to collect amounts owed on the account; or

(H) Provides you with the information necessary for you to compile and provide access to all of the consumer's on-line financial accounts at your Web site.

(ii) *Examples of loan rule.* You establish a customer relationship with a consumer who obtains a loan for personal, family, or household purposes when you:

(A) Originate the loan to the consumer and retain the servicing rights; or

(B) Purchase the servicing rights to the consumer's loan.

(d) *Existing customers.* When an existing customer obtains a new financial product or service from you that is to be used primarily for personal, family, or household purposes, you satisfy the initial notice requirements of paragraph (a) of this section as follows:

(1) You may provide a revised privacy notice, under § 313.8, that covers the customer's new financial product or service; or

(2) If the initial, revised, or annual notice that you most recently provided to that customer was accurate with respect to the new financial product or service, you do not need to provide a new privacy notice under paragraph (a) of this section.

(e) *Exceptions to allow subsequent delivery of notice.* (1) You may provide the initial notice required by paragraph (a)(1) of this section within a reasonable time after you establish a customer relationship if:

(i) Establishing the customer relationship is not at the customer's election; or

(ii) Providing notice not later than when you establish a customer relationship would substantially delay the customer's transaction and the customer agrees to receive the notice at a later time.

(2) *Examples of exceptions*—(i) *Not at customer's election.* Establishing a customer relationship is not at the customer's election if you acquire a customer's loan, or the servicing rights, from another financial institution and the customer does not have a choice about your acquisition.

(ii) *Substantial delay of customer's transaction.* Providing notice not later than when you establish a customer relationship would substantially delay the customer's transaction when:

(A) You and the individual agree over the telephone to enter into a customer relationship involving prompt delivery of the financial product or service; or

(B) You establish a customer relationship with an individual under a program authorized by Title IV of the Higher Education Act of 1965 (20 U.S.C. 1070 *et seq.*) or similar student loan programs where loan proceeds are disbursed promptly without prior communication between you and the customer.

(iii) *No substantial delay of customer's transaction.* Providing notice not later than when you establish a customer relationship would not substantially delay the customer's transaction when the relationship is initiated in person at your office or through other means by which the customer may view the notice, such as through a web site.

(f) *Delivery.* When you are required to deliver an initial privacy notice by this section, you must deliver it according to § 313.9. If you use a short-form initial notice for non-customers according to § 313.6(d), you may deliver your privacy notice according to § 313.6(d)(3).

§ 313.5 Annual privacy notice to customers required.

(a)(1) *General rule.* You must provide a clear and conspicuous notice to customers that accurately reflects your privacy policies and practices not less than annually during the continuation of the customer relationship. *Annually* means at least once in any period of 12 consecutive months during which that relationship exists. You may define the 12-consecutive-month period, but you must apply it to the customer on a consistent basis.

(2) *Example.* You provide a notice annually if you define the 12-consecutive-month period as a calendar year and provide the annual notice to the customer once in each calendar year following the calendar year in which you provided the initial notice. For example, if a customer opens an account on any day of year 1, you must provide an annual notice to that customer by December 31 of year 2.

(b)(1) *Termination of customer relationship.* You are not required to provide an annual notice to a former customer.

(2) *Examples.* Your customer becomes a former customer when:

(i) In the case of a closed-end loan, the customer pays the loan in full, you charge off the loan, or you sell the loan without retaining servicing rights;

(ii) In the case of a credit card relationship or other open-end credit relationship, you sell the receivables without retaining servicing rights;

(iii) In the case of credit counseling services, the customer has failed to make required payments under a debt management plan, has been notified that the plan is terminated, and you no longer provide any statements or notices to the customer concerning that relationship;

(iv) In the case of mortgage or vehicle loan brokering services, your customer has obtained a loan through you (and you no longer provide any statements or notices to the customer concerning that relationship), or has ceased using your services for such purposes;

(v) In the case of tax preparation services, you have provided and received payment for the service and no longer provide any statements or notices to the customer concerning that relationship;

(vi) In the case of providing real estate settlement services, at the time the customer completes execution of all documents related to the real estate closing, you have received payment, or you have completed all of your responsibilities with respect to the settlement, including filing documents on the public record, whichever is later.

(vii) In cases where there is no definitive time at which the customer relationship has terminated, you have not communicated with the customer about the relationship for a period of 12 consecutive months, other than to provide annual privacy notices or promotional material.

(c) *Special rule for loans.* If you do not have a customer relationship with a consumer under the special rule for loans in § 313.4(c)(2), then you need not provide an annual notice to that consumer under this section.

(d) *Delivery.* When you are required to deliver an annual privacy notice by this section, you must deliver it according to § 313.9.

§ 313.6 Information to be included in privacy notices.

(a) *General rule.* The initial, annual, and revised privacy notices that you provide under §§ 313.4, 313.5, and 313.8 must include each of the following items of information that applies to you or to the consumers to whom you send your privacy notice, in addition to any other information you wish to provide:

(1) The categories of nonpublic personal information that you collect;

(2) The categories of nonpublic personal information that you disclose;

(3) The categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information, other than those parties to whom you disclose information under §§ 313.14 and 313.15;

(4) The categories of nonpublic personal information about your former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your former customers, other than those parties to whom you disclose information under §§ 313.14 and 313.15;

(5) If you disclose nonpublic personal information to a nonaffiliated third party under § 313.13 (and no exception under §§ 313.14 or 313.15 applies to that disclosure), a separate statement of the categories of information you disclose and the categories of third parties with whom you have contracted;

(6) An explanation of the consumer's right under § 313.10(a) to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right at that time;

(7) Any disclosures that you make under section 603(d)(2)(A)(iii) of the Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);

(8) Your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and

(9) Any disclosure that you make under paragraph (b) of this section.

(b) *Description of nonaffiliated third parties subject to exceptions.* If you disclose nonpublic personal information to third parties as authorized under §§ 313.14 and 313.15, you are not required to list those exceptions in the initial or annual privacy notices required by §§ 313.4 and 313.5. When describing the categories with respect to those parties, you are required to state only that you make disclosures to other

nonaffiliated third parties as permitted by law.

(c) *Examples*—(1) *Categories of nonpublic personal information that you collect.* You satisfy the requirement to categorize the nonpublic personal information that you collect if you list the following categories, as applicable:

(i) Information from the consumer;

(ii) Information about the consumer's transactions with you or your affiliates;

(iii) Information about the consumer's transactions with nonaffiliated third parties; and

(iv) Information from a consumer reporting agency.

(2) *Categories of nonpublic personal information you disclose*—(i) You satisfy the requirement to categorize the nonpublic personal information that you disclose if you list the categories described in paragraph (e)(1) of this section, as applicable, and a few examples to illustrate the types of information in each category.

(ii) If you reserve the right to disclose all of the nonpublic personal information about consumers that you collect, you may simply state that fact without describing the categories or examples of the nonpublic personal information you disclose.

(3) *Categories of affiliates and nonaffiliated third parties to whom you disclose.* You satisfy the requirement to categorize the affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information if you list them using the following categories, as applicable, and a few applicable examples to illustrate the significant types of third parties covered in each category.

(i) Financial service providers, followed by illustrative examples such as mortgage bankers, securities broker-dealers, and insurance agents.

(ii) Non-financial companies, followed by illustrative examples such as retailers, magazine publishers, airlines, and direct marketers; and

(iii) Others, followed by examples such as nonprofit organizations.

(4) *Disclosures under exception for service providers and joint marketers.* If you disclose nonpublic personal information under the exception in § 313.13 to a nonaffiliated third party to market products or services that you offer alone or jointly with another financial institution, you satisfy the disclosure requirement of paragraph (a)(5) of this section if you:

(i) List the categories of nonpublic personal information you disclose, using the same categories and examples you used to meet the requirements of paragraph (a)(2) of this section, as applicable; and

(ii) State whether the third party is:

(A) A service provider that performs marketing services on your behalf or on behalf of you and another financial institution; or

(B) A financial institution with whom you have a joint marketing agreement.

(5) *Simplified notices.* If you do not disclose, and do not wish to reserve the right to disclose, nonpublic personal information about customers or former customers to affiliates or nonaffiliated third parties except as authorized under §§ 313.14 and 313.15, you may simply state that fact, in addition to the information you must provide under paragraphs (a)(1), (a)(8), (a)(9), and (b) of this section.

(6) *Confidentiality and security.* You describe your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information if you do both of the following:

(i) Describe in general terms who is authorized to have access to the information; and

(ii) State whether you have security practices and procedures in place to ensure the confidentiality of the information in accordance with your policy. You are not required to describe technical information about the safeguards you use.

(d) *Short-form initial notice with opt out notice for non-customers*—(1) You may satisfy the initial notice requirements in §§ 313.4(a)(2), 313.7(b), and 313.7(c) for a consumer who is not a customer by providing a short-form initial notice at the same time as you deliver an opt out notice as required in § 313.7.

(2) A short-form initial notice must:

(i) Be clear and conspicuous;

(ii) State that your privacy notice is available upon request; and

(iii) Explain a reasonable means by which the consumer may obtain that notice.

(3) You must deliver your short-form initial notice according to § 313.9. You are not required to deliver your privacy notice with your short-form initial notice. You instead may simply provide the consumer a reasonable means to obtain your privacy notice. If a consumer who receives your short-form notice requests your privacy notice, you must deliver your privacy notice according to § 313.9.

(4) *Examples of obtaining privacy notice.* You provide a reasonable means by which a consumer may obtain a copy of your privacy notice if you:

(i) Provide a toll-free telephone number that the consumer may call to request the notice; or

(ii) For a consumer who conducts business in person at your office, maintain copies of the notice on hand that you provide to the consumer immediately upon request.

(e) *Future disclosures.* Your notice may include:

(1) Categories of nonpublic personal information that you reserve the right to disclose in the future, but do not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom you reserve the right in the future to disclose, but to whom you do not currently disclose, nonpublic personal information.

(f) *Sample clauses.* Sample clauses illustrating some of the notice content required by this section are included in Appendix A of this part.

§ 313.7 Form of opt out notice to consumers; opt out methods.

(a) (1) *Form of opt out notice.* If you are required to provide an opt out notice under § 313.10(a), you must provide a clear and conspicuous notice to each of your consumers that accurately explains the right to opt out under that section. The notice must state:

(i) That you disclose or reserve the right to disclose nonpublic personal information about your consumer to a nonaffiliated third party;

(ii) That the consumer has the right to opt out of that disclosure; and

(iii) A reasonable means by which the consumer may exercise the opt out right.

(2) *Examples*—(i) *Adequate opt out notice.* You provide adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if you:

(A) Identify all of the categories of nonpublic personal information that you disclose or reserve the right to disclose, and all of the categories of nonaffiliated third parties to which you disclose the information, as described in § 313.6(a) (2) and (3) and state that the consumer can opt out of the disclosure of that information; and

(B) Identify the financial products or services that the consumer obtains from you, either singly or jointly, to which the opt out direction would apply.

(ii) *Reasonable opt out means.* You provide a reasonable means to exercise an opt out right if you:

(A) Designate check-off boxes in a prominent position on the relevant forms with the opt out notice;

(B) Include a reply form that includes the address to which the form should be mailed; or

(C) Provide an electronic means to opt out, such as a form that can be sent via

electronic mail or a process at your web site, if the consumer agrees to the electronic delivery of information; or

(D) Provide a toll-free telephone number that consumers may call to opt out.

(iii) *Unreasonable opt out means.* You *do not* provide a reasonable means of opting out if:

(A) The only means of opting out is for the consumer to write his or her own letter to exercise that opt out right; or

(B) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that you provided with the initial notice but did not include with the subsequent notice.

(iv) *Specific opt out means.* You may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

(b) *Same form as initial notice permitted.* You may provide the opt out notice together with or on the same written or electronic form as the initial notice you provide in accordance with § 313.4.

(c) *Initial notice required when opt out notice delivered subsequent to initial notice.* If you provide the opt out notice later than required for the initial notice in accordance with § 313.4, you must also include a copy of the initial notice with the opt out notice in writing or, if the consumer agrees, electronically.

(d) *Joint relationships*—(1) If two or more consumers jointly obtain a financial product or service from you, you may provide a single opt out notice, unless one or more of those consumers requests a separate opt out notice. Your opt out notice must explain how you will treat an opt out direction by a joint consumer (as explained in paragraph (d)(5)(ii)of this section).

(2) Any of the joint consumers may exercise the right to opt out. You may either:

(i) Treat an opt out direction by a joint consumer as applying to all of the associated joint consumers; or

(ii) Permit each joint consumer to opt out separately.

(3) If you permit each joint consumer to opt out separately, you must permit one of the joint consumers to opt out on behalf of all of the joint consumers.

(4) You may not require *all* joint consumers to opt out before you implement *any* opt out direction.

(5) *Example.* If John and Mary have a joint credit card account with you and arrange for you to send statements to John's address, you may do any of the following, but you must explain in your opt out notice which opt out policy you will follow:

(i) Send a single opt out notice to John's address, but you must accept an opt out direction from either John or Mary.

(ii) Treat an opt out direction by either John or Mary as applying to the entire account. If you do so, and John opts out, you may not require Mary to opt out as well before implementing John's opt out direction.

(iii) Permit John and Mary to make different opt out directions. If you do so,

(A) You must permit John and Mary to opt out for each other;

(B) If both opt out, you must permit both to notify you in a single response (such as on a form or through a telephone call); and

(C) If John opts out and Mary does not, you may only disclose nonpublic personal information about Mary, but not about John and not about John and Mary jointly.

(e) *Time to comply with opt out.* You must comply with a consumer's opt out direction as soon as reasonably practicable after you receive it.

(f) *Continuing right to opt out.* A consumer may exercise the right to opt out at any time.

(g) *Duration of consumer's opt out direction*—(1) A consumer's direction to opt out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.

(2) When a customer relationship terminates, the customer's opt out direction continues to apply to the nonpublic personal information that you collected during or related to that relationship. If the individual subsequently establishes a new customer relationship with you, the opt out direction that applied to the former relationship does not apply to the new relationship.

(h) *Delivery.* When you are required to deliver an opt out notice by this section, you must deliver it according to § 313.9.

§ 313.8 Revised privacy notices.

(a) *General rule.* Except as otherwise authorized in this part, you must not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice that you provided to that consumer under § 313.4, unless:

(1) You have provided to the consumer a clear and conspicuous revised notice that accurately describes your policies and practices;

(2) You have provided to the consumer a new opt out notice;

(3) You have given the consumer a reasonable opportunity, before you disclose the information to the nonaffiliated third party, to opt out of the disclosure; and

(4) the consumer does not opt out.

(b) *Examples*—(1) Except as otherwise permitted by §§ 313.13, 313.14, and 313.15, you must provide a revised notice before you:

(i) Disclose a new category of nonpublic personal information to any nonaffiliated third party;

(ii) Disclose nonpublic personal information to a new category of nonaffiliated third party; or

(iii) Disclose nonpublic personal information about a former customer to a nonaffiliated third party if that former customer has not had the opportunity to exercise an opt out right regarding that disclosure.

(2) A revised notice is not required if you disclose nonpublic personal information to a new nonaffiliated third party that you adequately described in your prior notice.

(c) *Delivery.* When you are required to deliver a revised privacy notice by this section, you must deliver it according to § 313.9.

§ 313.9 Delivering privacy and opt out notices.

(a) *How to provide notices.* You must provide any privacy notices and opt out notices, including short-form initial notices, that this part requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically.

(b)(1) *Examples of reasonable expectation of actual notice.* You may reasonably expect that a consumer will receive actual notice if you:

(i) Hand-deliver a printed copy of the notice to the consumer;

(ii) Mail a printed copy of the notice to the last known address of the consumer;

(iii) For the consumer who conducts transactions electronically, clearly and conspicuously post the notice on the electronic site and require the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular financial product or service;

(iv) For an isolated transaction with the consumer, such as an ATM transaction, post the notice on the ATM screen and require the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular financial product or service.

(2) *Examples of unreasonable expectation of actual notice.* You may *not,* however, reasonably expect that a consumer will receive actual notice of your privacy policies and practices if you:

(i) Only post a sign in your branch or office or generally publish

advertisements of your privacy policies and practices;

(ii) Send the notice via electronic mail to a consumer who does not obtain a financial product or service from you electronically.

(c) *Annual notices only.* You may reasonably expect that a customer will receive actual notice of your annual privacy notice if:

(1) The customer uses your web site to access financial products and services electronically and agrees to receive notices at the web site and you post your current privacy notice continuously in a clear and conspicuous manner on the web site; or

(2) The customer has requested that you refrain from sending any information regarding the customer relationship, and your current privacy notice remains available to the customer upon request.

(d) *Oral description of notice insufficient.* You may not provide any notice required by this part solely by orally explaining the notice, either in person or over the telephone.

(e) *Retention or accessibility of notices for customers*—(1) For customers only, you must provide the initial notice required by § 313.4(a)(1), the annual notice required by § 313.5(a), and the revised notice required by § 313.8 so that the customer can retain them or obtain them later in writing or, if the customer agrees, electronically.

(2) *Examples of retention or accessibility.* You provide a privacy notice to the customer so that the customer can retain it or obtain it later if you:

(i) Hand-deliver a printed copy of the notice to the customer;

(ii) Mail a printed copy of the notice to the last known address of the customer; or

(iii) Make your current privacy notice available on a web site (or a link to another web site) for the customer who obtains a financial product or service electronically and agrees to receive the notice at the web site.

(f) *Joint notice with other financial institutions.* You may provide a joint notice from you and one or more of your affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to you and the other institutions.

(g) *Joint relationships.* If two or more consumers jointly obtain a financial product or service from you, you may satisfy the initial, annual, and revised notice requirements of §§ 313.4(a), 313.5(a), and 313.8(a) by providing one notice to those consumers jointly, unless one or more of those consumers requests separate notices.

Subpart B—Limits on Disclosures

§ 313.10 Limits on disclosure of nonpublic personal information to nonaffiliated third parties.

(a)(1) *Conditions for disclosure.* Except as otherwise authorized in this part, you may not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party unless:

(i) You have provided to the consumer an initial notice as required under § 313.4;

(ii) You have provided to the consumer an opt out notice as required in § 313.7;

(iii) You have given the consumer a reasonable opportunity, before you disclose the information to the nonaffiliated third party, to opt out of the disclosure; and

(iv) The consumer does not opt out.

(2) *Opt out definition.* Opt out means a direction by the consumer that you not disclose nonpublic personal information about that consumer to a nonaffiliated third party, other than as permitted by §§ 313.13, 313.14, and 313.15.

(3) *Examples of reasonable opportunity to opt out.* You provide a consumer with a reasonable opportunity to opt out if:

(i) *By mail.* You mail the notices required in paragraph (a)(1) of this section to the consumer and allow the consumer to opt out by mailing a form, calling a toll-free telephone number, or any other reasonable means within 30 days from the date you mailed the notices.

(ii) *By electronic means.* A customer opens an on-line account with you and agrees to receive the notices required in paragraph (a)(1) of this section electronically, and you allow the customer to opt out by any reasonable means within 30 days after the date that the customer acknowledges receipt of the notices in conjunction with opening the account.

(iii) *Isolated transaction with consumer.* For an isolated transaction, such as the purchase of a money order by a consumer, you provide the consumer with a reasonable opportunity to opt out if you provide the notices required in paragraph (a)(1) of this section at the time of the transaction and request that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

(b) *Application of opt out to all consumers and all nonpublic personal information*—(1) You must comply with this section, regardless of whether you and the consumer have established a customer relationship

(2) Unless you comply with this section, you may not, directly or through any affiliate, disclose any nonpublic personal information about a consumer that you have collected, regardless of whether you collected it before or after receiving the direction to opt out from the consumer.

(c) *Partial opt out.* You may allow a consumer to select certain nonpublic personal information or certain nonaffiliated third parties with respect to which the consumer wishes to opt out.

§ 313.11 Limits on redisclosure and reuse of information.

(a)(1) *Information you receive under an exception.* If you receive nonpublic personal information from a nonaffiliated financial institution under an exception in § 313.14 or 313.15 of this part, your disclosure and use of that information is limited as follows:

(i) You may disclose the information to the affiliates of the financial institution from which you received the information;

(ii) You may disclose the information to your affiliates, but your affiliates may, in turn, disclose and use the information only to the extent that you may disclose and use the information; and

(iii) You may disclose and use the information pursuant to an exception in § 313.14 or 313.15 in the ordinary course of business to carry out the activity covered by the exception under which you received the information.

(2) *Example.* If you receive a customer list from a nonaffiliated financial institution in order to provide account processing services under the exception in § 313.14(a), you may disclose that information under any exception in § 313.14 or 313.15 in the ordinary course of business in order to provide those services. You could also disclose that information in response to a properly authorized subpoena. You could not disclose that information to a third party for marketing purposes or use that information for your own marketing purposes.

(b)(1) *Information you receive outside of an exception.* If you receive nonpublic personal information from a nonaffiliated financial institution other than under an exception in § 313.14 or 313.15 of this part, you may disclose the information only:

(i) To the affiliates of the financial institution from which you received the information;

(ii) To your affiliates, but your affiliates may, in turn, disclose the information only to the extent that you can disclose the information; and

(iii) To any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which you received the information.

(2) *Example.* If you obtain a customer list from a nonaffiliated financial institution outside of the exceptions in § 313.14 and 313.15:

(i) You may use that list for your own purposes; and

(ii) You may disclose that list to another nonaffiliated third party only if the financial institution from which you purchased the list could have lawfully disclosed the list to that third party. That is, you may disclose the list in accordance with the privacy policy of the financial institution from which you received the list, as limited by the opt out direction of each consumer whose nonpublic personal information you intend to disclose, and you may disclose the list in accordance with an exception in § 313.14 or 313.15, such as to your attorneys or accountants.

(c) *Information you disclose under an exception.* If you disclose nonpublic personal information to a nonaffiliated third party under an exception in § 313.14 or 313.15 of this part, the third party may disclose and use that information only as follows:

(1) The third party may disclose the information to your affiliates;

(2) The third party may disclose the information to its affiliates, but its affiliates may, in turn, disclose and use the information only to the extent that the third party may disclose and use the information; and

(3) The third party may disclose and use the information pursuant to an exception in § 313.14 or 313.15 in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

(d) *Information you disclose outside of an exception.* If you disclose nonpublic personal information to a nonaffiliated third party other than under an exception in § 313.14 or 313.15 of this part, the third party may disclose the information only:

(1) To your affiliates;

(2) To its affiliates, but its affiliates, in turn, may disclose the information only to the extent the third party can disclose the information; and

(3) To any other person, if the disclosure would be lawful if you made it directly to that person.

§ 313.12 Limits on sharing account number information for marketing purposes.

(a) *General prohibition on disclosure of account numbers.* You must not, directly or through an affiliate, disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a consumer's credit card account, deposit account, or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.

(b) *Exceptions.* Paragraph (a) of this section does not apply if you disclose an account number or similar form of access number or access code:

(1) To your agent or service provider solely in order to perform marketing for your own products or services, as long as the agent or service provider is not authorized to directly initiate charges to the account; or

(2) To a participant in a private label credit card program or an affinity or similar program where the participants in the program are identified to the customer when the customer enters into the program.

(c) *Examples*—(1) *Account number.* An account number, or similar form of access number or access code, does not include a number or code in an encrypted form, as long as you do not provide the recipient with a means to decode the number or code.

(2) *Transaction account.* A transaction account is an account other than a deposit account or a credit card account. A transaction account does not include an account to which third parties cannot initiate charges.

Subpart C—Exceptions

§ 313.13 Exception to opt out requirements for service providers and joint marketing.

(a) *General rule.* (1) The opt out requirements in §§ 313.7 and 313.10 do not apply when you provide nonpublic personal information to a nonaffiliated third party to perform services for you or functions on your behalf, if you:

(i) Provide the initial notice in accordance with § 313.4; and

(ii) Enter into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which you disclosed the information, including use under an exception in § 313.14 or 313.15 in the ordinary course of business to carry out those purposes.

(2) *Example.* If you disclose nonpublic personal information under this section to a financial institution with which you perform joint marketing, your contractual agreement with that institution meets the requirements of paragraph (a)(1)(ii) of this section if it prohibits the institution from disclosing or using the nonpublic personal information except as necessary to carry out the joint marketing or under an exception in § 313.14 or 313.15 in the ordinary course of business to carry out that joint marketing.

(b) *Service may include joint marketing.* The services a nonaffiliated third party performs for you under paragraph (a) of this section may include marketing of your own products or services or marketing of financial products or services offered pursuant to joint agreements between you and one or more financial institutions.

(c) *Definition of joint agreement.* For purposes of this section, joint agreement means a written contract pursuant to which you and one or more financial institutions jointly offer, endorse, or sponsor a financial product or service.

§ 313.14 Exceptions to notice and opt out requirements for processing and servicing transactions.

(a) *Exceptions for processing transactions at consumer's request.* The requirements for initial notice in § 313.4(a)(2), for the opt out in §§ 313.7 and 313.10, and for service providers and joint marketing in § 313.13 do not apply if you disclose nonpublic personal information as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or in connection with:

(1) Servicing or processing a financial product or service that a consumer requests or authorizes;

(2) Maintaining or servicing the consumer's account with you, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or

(3) A proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer.

(b) *Necessary to effect, administer, or enforce a transaction* means that the disclosure is:

(1) Required, or is one of the lawful or appropriate methods, to enforce your rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or

(2) Required, or is a usual, appropriate or acceptable method:

(i) To carry out the transaction or the product or service business of which the transaction is a part, and record, service, or maintain the consumer's account in the ordinary course of providing the financial service or financial product;

(ii) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;

(iii) To provide a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product to the consumer or the consumer's agent or broker;

(iv) To accrue or recognize incentives or bonuses associated with the transaction that are provided by you or any other party;

(v) To underwrite insurance at the consumer's request or for reinsurance purposes, or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating, or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects, or as otherwise required or specifically permitted by Federal or State law;

(vi) In connection with:

(A) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited, or otherwise paid using a debit, credit, or other payment card, check, or account number, or by other payment means;

(B) The transfer of receivables, accounts, or interests therein; or

(C) The audit of debit, credit, or other payment information.

§ 313.15 Other exceptions to notice and opt out requirements.

(a) *Exceptions to opt out requirements.* The requirements for initial notice in § 313.4(a)(2), for the opt out in §§ 313.7 and 313.10, and for service providers and joint marketing in § 313.13 do not apply when you disclose nonpublic personal information:

(1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;

(2)(i) To protect the confidentiality or security of your records pertaining to the consumer, service, product, or transaction;

(ii) To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;

(iii) For required institutional risk control or for resolving consumer disputes or inquiries;

(iv) To persons holding a legal or beneficial interest relating to the consumer; or

(v) To persons acting in a fiduciary or representative capacity on behalf of the consumer;

(3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating you, persons that are assessing your compliance with industry standards, and your attorneys, accountants, and auditors;

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 *et seq.*), to law enforcement agencies (including a federal functional regulator, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a State insurance authority, with respect to any person domiciled in that insurance authority's State that is engaged in providing insurance, and the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;

(5)(i) To a consumer reporting agency in accordance with the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*), or

(ii) From a consumer report reported by a consumer reporting agency;

(6) In connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or

(7)(i) To comply with Federal, State, or local laws, rules and other applicable legal requirements;

(ii) To comply with a properly authorized civil, criminal, or regulatory investigation, or subpoena or summons by Federal, State, or local authorities; or

(iii) To respond to judicial process or government regulatory authorities having jurisdiction over you for examination, compliance, or other purposes as authorized by law.

(b) *Examples of consent and revocation of consent.* (1) A consumer may specifically consent to your disclosure to a nonaffiliated insurance company of the fact that the consumer has applied to you for a mortgage so that the insurance company can offer homeowner's insurance to the consumer.

(2) A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under § 313.7(f).

Subpart D—Relation to Other Laws; Effective Date

§ 313.16 Protection of Fair Credit Reporting Act.

Nothing in this part shall be construed to modify, limit, or supersede the operation of the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*), and no inference shall be drawn on the basis of the provisions of this part regarding whether information is transaction or experience information under section 603 of that Act.

§ 313.17 Relation to State laws.

(a) *In general.* This part shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such State statute, regulation, order, or interpretation is inconsistent with the provisions of this part, and then only to the extent of the inconsistency.

(b) *Greater protection under State law.* For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this part if the protection such statute, regulation, order, or interpretation affords any consumer is greater than the protection provided under this part, as determined by the Commission on its own motion or upon the petition of any interested party, after consultation with the applicable federal functional regulator or other authority.

§ 313.18 Effective date; transition rule.

(a) *Effective date.* (1) *General rule.* This part is effective November 13, 2000. In order to provide sufficient time for you to establish policies and systems to comply with the requirements of this part, the Commission has extended the time for compliance with this part until July 1, 2001.

(2) *Exception.* This part is not effective as to any institution that is significantly engaged in activities that the Federal Reserve Board determines, after November 12, 1999, (pursuant to its authority in Section 4(k)(1–3) of the Bank Holding Company Act), are activities that a financial holding company may engage in, until the Commission so determines.

(b)(1) *Notice requirement for consumers who are your customers on the compliance date.* By July 1, 2001, you must have provided an initial notice, as required by § 313.4, to consumers who are your customers on July 1, 2001.

(2) *Example.* You provide an initial notice to consumers who are your customers on July 1, 2001, if, by that

date, you have established a system for providing an initial notice to all new customers and have mailed the initial notice to all your existing customers.

(c) *Two-year grandfathering of service agreements.* Until July 1, 2002, a contract that you have entered into with a nonaffiliated third party to perform services for you or functions on your behalf satisfies the provisions of § 313.13(a)(1) of this part, even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as you entered into the contract on or before July 1, 2000.

Appendix A to Part 313—Sample Clauses

Financial institutions, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets and income, and information from a consumer reporting agency, may give rise to obligations under the Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A–1—Categories of Information You Collect (All Institutions)

You may use this clause, as applicable, to meet the requirement of § 313.6(a)(1) to describe the categories of nonpublic personal information you collect.

Sample Clause A–1

We collect nonpublic personal information about you from the following sources:

- Information we receive from you on applications or other forms;
- Information about your transactions with us, our affiliates, or others; and
- Information we receive from a consumer reporting agency.

A–2—Categories of Information You Disclose (Institutions That Disclose Outside of the Exceptions)

You may use one of these clauses, as applicable, to meet the requirement of § 313.6(a)(2) to describe the categories of nonpublic personal information you disclose. You may use these clauses if you disclose nonpublic personal information other than as permitted by the exceptions in §§ 313.13, 313.14, and 313.15.

Sample Clause A–2, Alternative 1

We may disclose the following kinds of nonpublic personal information about you:

- Information we receive from you on applications or other forms, such as [*provide illustrative examples, such as ''your name, address, social security number, assets, and income''*];
- Information about your transactions with us, our affiliates, or others, such as [*provide illustrative examples, such as ''your account balance, payment history, parties to transactions, and credit card usage''*]; and
- Information we receive from a consumer reporting agency, such as [*provide illustrative examples, such as ''your creditworthiness and credit history''*].

Sample Clause A–2, Alternative 2

We may disclose all of the information that we collect, as described [*describe location in the notice, such as ''above'' or ''below''*].

A–3—Categories of Information You Disclose and Parties to Whom You Disclose (Institutions That Do Not Disclose Outside of the Exceptions)

You may use this clause, as applicable, to meet the requirements of §§ 313.6(a)(2), (3), and (4) to describe the categories of nonpublic personal information about customers and former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose. You may use this clause if you do not disclose nonpublic personal information to any party, other than as permitted by the exceptions in §§ 313.14, and 313.15.

Sample Clause A–3

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.

A–4—Categories of Parties to Whom You Disclose (Institutions That Disclose Outside of the Exceptions)

You may use this clause, as applicable, to meet the requirement of § 313.6(a)(3) to describe the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information. You may use this clause if you disclose nonpublic personal information other than as permitted by the exceptions in §§ 313.13, 313.14, and 313.15, as well as when permitted by the exceptions in §§ 313.14, and 313.15.

Sample Clause A–4

We may disclose nonpublic personal information about you to the following types of third parties:

- Financial service providers, such as [*provide illustrative examples, such as ''mortgage bankers, securities broker-dealers, and insurance agents''*];
- Non-financial companies, such as [*provide illustrative examples, such as ''retailers, direct marketers, airlines, and publishers''*]; and
- Others, such as [*provide illustrative examples, such as ''non-profit organizations''*].

We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.

A–5—Service Provider/Joint Marketing Exception

You may use one of these clauses, as applicable, to meet the requirements of § 313.6(a)(5) related to the exception for service providers and joint marketers in § 313.13. If you disclose nonpublic personal information under this exception, you must describe the categories of nonpublic personal information you disclose and the categories of third parties with whom you have contracted.

Sample Clause A–5, Alternative 1

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements:

- Information we receive from you on applications or other forms, such as [*provide illustrative examples, such as ''your name, address, social security number, assets, and income''*];
- Information about your transactions with us, our affiliates, or others, such as [*provide illustrative examples, such as ''your account balance, payment history, parties to transactions, and credit card usage''*]; and
- Information we receive from a consumer reporting agency, such as [*provide illustrative examples, such as ''your creditworthiness and credit history''*].

Sample Clause A–5, Alternative 2

We may disclose all of the information we collect, as described [*describe location in the notice, such as ''above'' or ''below''*] to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

A–6—Explanation of Opt Out Right (Institutions that Disclose Outside of the Exceptions)

You may use this clause, as applicable, to meet the requirement of § 313.6(a)(6) to provide an explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. You may use this clause if you disclose nonpublic personal information other than as permitted by the exceptions in §§ 313.13, 313.14, and 313.15.

Sample Clause A–6

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [*describe a reasonable means of opting out, such as ''call the following toll-free number: (insert number)''*].

A–7—Confidentiality and Security (All Institutions)

You may use this clause, as applicable, to meet the requirement of § 313.6(a)(8) to describe your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A–7

We restrict access to nonpublic personal information about you to [*provide an appropriate description, such as ''those employees who need to know that information to provide products or services to you''*]. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

By direction of the Commission.

Approved by the Commission on May 12, 2000.

Donald S. Clark,

Secretary.

[FR Doc. 00–12755 Filed 5–23–00; 8:45 am]

BILLING CODE 6750–01–P

Transferring European Personal Data Across Borders

Robert L. Rothman, Chief Privacy Officer
General Motors Corporation

Presentation Overview

- European Regulatory Background
- Data Transfer Derogations: Pro's and Con's

GM's Data Transfer Issue

- The EU Commission's Directive 95/46/EC pertaining to the protection of personal information went into effect in October, 1998.
- European Union member countries were required to adopt Directive provisions into their national laws as minimum standards, but were allowed to include more protection than Directive requires.
- Directive prohibits transferring personal data outside the EU unless it is transferred to a country deemed to have "adequate privacy" rules/laws or the transfer falls under a "derogation" (an exception).
- For various business reasons, companies need to transfer employee and consumer personal information from European Union countries to the United States and other non-European Union countries.

What is Personal Data?

- Personal Data is "any information relating to an identified or identifiable natural person."
  - Extremely broad – includes business contact information.
  - "Sensitive Personal Data" – special category of Personal Information relating to racial or ethnic origin, political opinion, religious belief, trade union membership, health, or sex life. Stricter rules apply.

Processing Personal Information in Europe

Individual European country laws require that businesses processing personal information (defined to include collection, recording, storage, retrieval, destruction, transfer etc.) must:

- Register personal information processing with respective data protection authorities.
- Meet one of the Article 7 criteria for making data processing legitimate.
- Comply with the details of the European Directive principles that relate to:
  - Notice
  - Onward Transfer
  - Choice
  - Security
  - Data Integrity
  - Access
  - Enforcement

Article 7 Criteria for Making Data Processing Legitimate

- Data subject gives unambiguous consent.
- Processing necessary for performance of contract to which data subject is party.
- Processing is necessary for compliance with legal obligation to which controller is subject.
- Processing is necessary to protect vital interest of data subject.
- Processing is necessary for performance of task carried out in public interest or exercise of official authority.
- Processing is necessary for purposes of the legitimate interests pursued by controller or by the third party/ies to whom data are disclosed, except where such interests are overridden by the interest for fundamental rights and freedoms on the data subject that require protection.

Fines and Penalties - Examples

- Local data protection authorities have right to audit, investigate and prosecute.
- Companies can be fined.
- Directors can be prosecuted.
- Individual employees can be prosecuted.
- GM can be ordered to stop processing data in certain ways.
- Any customer, employee or local data protection official can demand company prove that processing has been lawful.

Adequate Third Countries

The following non-EU member countries have adequate data protection laws:

•Switzerland

•Norway

•Iceland

•Liechtenstein

•Hungary

•Canada (consumer data)

•Argentina

•Also, transfers to affiliated entities in the U. S. which have subscribed to Safe Harbor Principles.

Data Transfer Derogations

Data Transfer Derogations

To be able to transfer personal information outside of the EU, the data transfer must meet one of the Directive Article 26 derogations:

- Data subject has given unambiguous consent.
- Transfer is necessary for performance of contract.
- Transfer is necessary or legally required for public interest.
- Transfer is necessary to protect vital interests of data subject.
- Transfer is made from public register.

Derogations (continued)

- Meet other Data Transfer Derogations:
  - Safe Harbor – U. S. companies may self-certify that they are in compliance with Safe Harbor requirements agreed upon by EU Commission and Department of Commerce.
  - Model Contracts – adopt standard contracts between EU transferor and third country transferees or processors.
  - Ad Hoc Contracts – contracts between EU transferor and third country transferees approved by individual countries' data protection authorities.
  - Codes of Conduct – global policy substantively similar to model contracts which have been approved by the individual countries' data protection authorities.

Consent

Requirements

- Must provide complete notice as to how data will be processed.
  - What data is being collected.
  - How it will be used.
  - With whom it will be shared.
- Must obtain data subject's unambiguous consent to transfer personal information and for subsequent use of personal information.

Advantages

- Eliminates restrictions on data transfers.
- Data subject provides direct input.

Consent (continued)

Challenges

- Data subject may withhold or revoke consent which requires the availability of alternate processes.
- Securing consent of employees may require input of works councils.
- May not be an option for employee data going forward as many question employee's ability to withhold consent – legislation pending to eliminate consent as a basis of transfer in the employment context.
- Some countries require a data transfer permit issued by their data protection authority which may additionally require an agreement that binds initial and subsequent transferees to handle data according to certain privacy principles, irrespective of consent given (e.g., Portugal, Hungary, Switzerland, Spain).
- Administrative burden keeping track of consents.

Safe Harbor

- Safe Harbor requires certification by U.S. entity and compliance with Safe Harbor Principles.
- Certification may be made for all or selected personal information flows.

Safe Harbor (continued)

Certification

- Corporate officer in U. S. must register with Dept. of Commerce that the corporation adheres to Safe Harbor Privacy Principles.
- Registrant must:
  - Describe the way corporation uses personal information.
  - Summarize privacy policies and indicate where they are available for public viewing.
  - Indicate how corporation intends to verify compliance with Safe Harbor Principles and the enforcement procedures to which it will submit.
- Corporate official must recertify on a 12-month basis.
- Certification evidenced by publication on U. S. Commerce Department's web site (www.export.gov/safeharbor/).

Safe Harbor (continued)

Notice

Must inform data subjects about:

- Purposes for collecting/using their personal information.
- How to contact organization with inquiries or complaints.
- Third parties or categories of third parties to whom personal information disclosed.
- Choices organization offers to data subjects for limiting use and disclosure of personal information.

Choice

- Must offer data subjects opportunity to opt-out of data sharing with third parties or for subsequent uses of personal information (e.g., future marketing).
- Affirmative opt-in must be provided for Sensitive Personal Data.

Safe Harbor (continued)

Onward Transfer From U.S. Entity to Non-U.S. Entity in Inadequate Country

- Must apply notice and choice principles.
- Requires contract obligating any further transferees to comply with Safe Harbor principles.

Security

- Organizations must take reasonable precautions to protect personal information from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

Data Integrity

- Organizations may not process personal information in ways incompatible with purposes for which it was collected or subsequently authorized by data subject.
- Ensure that data is reliable for its intended use, accurate, complete, and current.

Safe Harbor (continued)

Access

- Data subjects must be provided with access to personal information an organization holds and be able to correct, amend or delete where inaccurate.

Enforcement

- Must have independent recourse mechanisms so individual complaints and disputes can be investigated and resolved.
- Must have procedures to verify that Safe Harbor commitments have been implemented.
- Must have obligations to remedy problems arising out of failure to comply with Safe Harbor principles.
- With respect to human resources data, dispute resolution mechanism has to be data protection authority of the country in which the data subject is located.

Safe Harbor (continued)

Advantages

- No EU member can challenge data transfer.
- Prior approval of data transfer waived/automatically granted.
- Slightly more liberal rules than compliance with EU Directive.

Safe Harbor (continued)

Challenges

- Must comply with 7 Safe Harbor Principles, including choice, access and security; thus, employee can still object to transfer.
- Must agree to "cooperate" with European data protection authorities with respect to employee personal information – meaning not yet clear.
- Not available for financial data (i.e., Financial Services companies).
- Violations would subject company to suits by U. S. Federal Trade Commission.
- Only applies to EU member countries – not other countries with EU-type data protection laws such as Switzerland and Hungary.
- May require business and system process changes and modifications.
- Would need global contract to address onward transfer principle compliance, particularly in the context of U. S.-hosted databases.

Model Contracts

Requirements

- Data may be transferred to inadequate country where transferring entity enters into EU standard contract with receiving entity.
- Personal data may only be collected for specified, explicit, and legitimate purposes.
- Data controller must:
  - Inform data subjects about purposes of collection, identity of controller, and countries that personal information will be transferred to.
  - Provide right of access to personal information and opportunity to correct.
  - Provide appropriate remedies for breach directly to data subjects including compensation or damages through courts.

Model Contracts (continued)

Advantages

- Would eliminate prior approval in several countries.
- Will work for financial data.

Challenges

- Company must submit itself to the jurisdiction of individual countries.
- Joint and several liability between data exporter in Europe and data importer in "inadequate" country.
- Data subjects treated as third party beneficiaries to contract and may enforce contract provisions and request costly mediation.
- Large number of contracts may be required between various transferring and receiving entities in a multinational company.
- Must foresee all categories of data to be transferred and include in contract.
- Requires notification to Data Protection Authorities.

Ad Hoc Contracts

Requirements

- Must specify how transferring and receiving entities handle personal information.
- Approval of data protection authority in transferring entity's country.

Advantages

- Same as model contracts.

Challenges

- Data protection authorities generally not approving ad hoc agreements unless substantially similar to model contract.
- Same disadvantages as model contracts, but additionally would require prior approval of data protection authorities of countries from which personal information is to be exported.

Codes of Conduct

Requirements

- Company can develop its own code of data privacy.
- Would need to address Directive data privacy principles.

Advantages

- Would avoid the numerous contracts required under model or ad hoc contracts.

Challenges

- Would need to be substantively similar to the model contract.
- Must be approved by data protection authority in each country where data is to be exported to a third country.
- Enterprise must adopt the code and comply with the provisions; may require approval of boards of many companies.

Other Derogations

•Transfer is necessary for the performance or conclusion of a contract.

- These transfers must meet the necessity test – all of the data transferred must be necessary for the performance of the contract (e.g., purchase of an airline ticket)
- If non-essential data are transferred or if the purpose is not the performance of the contract (e.g., follow-up marketing), the exemption is lost.
- Very narrowly construed.

•Transfer is required on important public interest grounds or in defense of a legal claim.

- The transfer must be for important public interests (e.g., transfer between social security and tax administrations) – not merely a simple public interest justification.
- To defend a claim, the context (e.g., an international lawsuit) warrants transfer.

Other Derogations (continued)

Transfer is necessary to protect the vital interests of the data subject.

- Transfers may only be those necessary to prevent injury or other damage to data subject's health or serious loss or damage to data subject's property.
  - Greece only allows these transfers when data subject is incapable of giving his or her consent.
  - Austria only allows these transfers when time is so urgent, a transfer permit cannot be timely obtained.
- Transfer is made from a public register.
  - Intention is that where a register is available for public consultation, a person who has the right to consult such register that is in a third country should be permitted to access the information in the register.
  - However, Recital 58 makes it clear that the entire registers or categories in registers should not be permitted to be transferred under this exemption.

Privacy Hypothetical

Assess and evaluate the personal data practices with respect to the fact pattern below.

American Company ("American") based in San Francisco is an up-and-coming manufacturer that sells directly to the consumer as well as to businesses. American Co. has two main products. The first is a consumer marketed Never Get Sick Again ("NGSA") tank that consumers submerse themselves into at home. The NGSA is also sold to businesses that add additional enhancements and then re-sell under private labels. That version is the NGSA II. It is claimed that the NGSA will cure all medical illnesses.

Consumers can log onto American's website (www.NGSA.com) and learn more about NGSA as well as purchase the NGSA. Upon purchase and installation, which is provided by a third party, Install Company ("Install"), consumers can then log onto the web and view a complete status of their health statistics 24 hours a day. In less than two hours, Install can set up the NGSA and get the consumer an account online, with user name and password, so they are fully operational.

American specializes in the manufacturing of the NGSA and does not have the technical expertise in-house to build a server farm to store the consumer data. American contracts with Computer Company ("Computer"), located in New York, to build and maintain at Computer's home office the networked servers that store the medical information of consumers that links to the individual consumer's NGSA information. Computer is a separately owned company and not affiliated with American.

Sales are slumping and consumer research shows that most consumers want the product, but cannot get a loan to cover the costly $10,000 price tag. American decides that it will offer financing through a newly created, wholly-owned subsidiary called Money Company ("Money"). The interface is simple -- consumers on the American website simply click on a financing link and are taken to the financing center. From there, they complete the necessary financial forms and submit. American provides the necessary information about the consumer to Money, and Money informs the consumer if they are approved for financing and informs American to complete and ship the NGSA.

In the background, Money works with Credit Company ("Credit") to review the credit worthiness and other demographic indicia to help Money decide whether to provide the financing. Money sends Credit the

application the consumers fill out, and Credit provides a report back to Money.

In an effort to maximize profit in a tough market, American decides that it will enter the home mortgage business and specifically target the refinancing opportunities because of low interest rates. American opens a wholly-owned subsidiary called Home Refinance Company ("Refi"). To kick-start business, American transmits to Refi the names of customers who qualify with Money for the NGSA financing. In order to avoid the expense of purchasing costly servers, Refi hires another company – Data Server – to store and arrange all consumer data at Data Server's home office.

After a year of successful growth in the United States, American realizes that the U.S. underwater healthcare market is absolutely saturated and the future lies in expanding overseas. In a competitive coup that is the talk of the entire submersible health care industry, American acquires 100% of the equity of its largest European competitor, the London-based Big Ben Limited ("Big Ben"). Big Ben has subsidiaries throughout Europe. To maximize efficiencies, American migrates all of Big Ben's European consumer data to American's brand new global centralized database in San Francisco, recently established after having terminated its relationship with Computer for questionable privacy practices.

Unfortunately, American is now struggling, partly because it grew too fast but also because it cannot manage its vast employee base efficiently. In an effort to save a sinking ship, American hires Infrastructure Company Ltd. in Bangalore, India ("Infra") to create a centralized database to manage the HR, payroll, and benefits databases for all employees globally, as well as institute and keep up-to-date the new global picture organization chart program. Additionally, Infra's highly educated but low cost management team will make decisions on hiring and firing and promotions and benefits centrally in Bangalore, thereby eliminating HR inconsistencies and leading to a truly equitable global organization.

Sadly, even the Bangalore efforts do not lead to a turnaround, and the ship is still sinking at American. American fires the U.S. marketing manager who rang all those false alarm bells about the U.S. market being saturated and decides to concentrate on U.S. sales. American hires ten summer marketing interns to search the Internet for email addresses and then begins to send email to those consumers across the U.S. with the message, "NGSA will save your life; go to www.NGSA.com and Never Get Sick Again."

American turns the tide and is now clicking on all cylinders. The marketing campaign works and the company is in great shape. However, shortly thereafter, American sees the following appear on the home page of www.NGSA.com, "I own you; I have access to your computers and all of your systems." American determines this is not an April Fool's joke and quickly learns that their website has been hacked. As it turns out, the culprit was an ex-employee who logged into the internal database with her old employee id and password.

CALIFORNIA BUSINESS AND PROFESSIONS CODE SECTION 17538.4 (including 2002 amendments)

§ 17538.4.

(a) No person or entity conducting business in this state shall electronically mail (e-mail) or cause to be e-mailed documents containing unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit unless that person or entity establishes a toll-free telephone number or valid sender operated return e-mail address that the recipient of the unsolicited documents may call or e-mail to notify the sender not to e-mail any further unsolicited documents.

(b) All unsolicited e-mailed documents subject to this section shall include a statement informing the recipient of the toll-free telephone number that the recipient may call, or a valid return address to which the recipient may write or e-mail, as the case may be, notifying the sender not to e-mail the recipient any further unsolicited documents to the e-mail address, or addresses, specified by the recipient.

The statement shall be the first text in the body of the message and shall be of the same size as the majority of the text of the message.

(c) Upon notification by a recipient of his or her request not to receive any further unsolicited e-mailed documents, no person or entity conducting business in this state shall e-mail or cause to be e-mailed any unsolicited documents to that recipient.

(d) This section shall apply when the unsolicited e-mailed documents are delivered to a California resident via an electronic mail service provider's service or equipment located in this state. For these purposes "electronic mail service provider" means any business or organization qualified to do business in this state that provides individuals, corporations, or other entities the ability to send or receive electronic mail through equipment located in this state and that is an intermediary in sending or receiving electronic mail.

(e) As used in this section, "unsolicited e-mailed documents" means any e-mailed document or documents consisting of advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit that meet both of the following requirements:

(1) The documents are addressed to a recipient with whom the initiator does not have an existing business or personal relationship.

(2) The documents are not sent at the request of, or with the express consent of, the recipient.

(f) As used in this section, "e-mail" or "cause to be e-mailed" does not include or refer to the transmission of any documents by a telecommunications utility or Internet service provider to the extent that the telecommunications utility or Internet service provider merely carries that transmission over its network.

(g) In the case of e-mail that consists of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit the subject line of each and every message shall include "ADV:" as the first four characters. If these messages contain information that consists of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit, that may only be viewed, purchased, rented, leased, or held in possession by an individual 18 years of age and older, the subject line of each and every message shall include "ADV:ADLT" as the first eight characters.

(h) An employer who is the registered owner of more than one e-mail address may notify the person or entity conducting business in this state e-mailing or causing to be e-mailed, documents consisting of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit of the desire to cease e-mailing on behalf of all of the employees who may use employer-provided and employer-controlled e-mail addresses.

(i) This section, or any part of this section, shall become inoperative on and after the date that federal law is enacted that prohibits or otherwise regulates the transmission of unsolicited advertising by electronic mail (e-mail).

CALIFORNIA BUSINESS AND PROFESSIONS CODE SECTION 17538.45

§ 17538.45.

(a) For purposes of this section, the following words have the following meanings:

(1) "Electronic mail advertisement" means any electronic mail message, the principal purpose of which is to promote, directly or indirectly, the sale or other distribution of goods or services to the recipient.

(2) "Unsolicited electronic mail advertisement" means any electronic mail advertisement that meets both of the following requirements:

(A) It is addressed to a recipient with whom the initiator does not have an existing business or personal relationship.
(B) It is not sent at the request of or with the express consent of the recipient.

(3) "Electronic mail service provider" means any business or organization qualified to do business in California that provides registered users the ability to send or receive electronic mail through equipment located in this state and that is an intermediary in sending or receiving electronic mail.

(4) "Initiation" of an unsolicited electronic mail advertisement refers to the action by the initial sender of the electronic mail advertisement. It does not refer to the actions of any intervening electronic mail service provider that may handle or retransmit the electronic message.

(5) "Registered user" means any individual, corporation, or other entity that maintains an electronic mail address with an electronic mail service provider.

(b) No registered user of an electronic mail service provider shall use or cause to be used that electronic mail service provider's equipment located in this state in violation of that electronic mail service provider's policy prohibiting or restricting the use of its service or equipment for the initiation of unsolicited electronic mail advertisements.

(c) No individual, corporation, or other entity shall use or cause to be used, by initiating an unsolicited electronic mail advertisement, an electronic mail service provider's equipment located in this state in violation of that electronic mail service provider's policy prohibiting or restricting the use of its equipment to deliver unsolicited electronic mail advertisements to its registered users.

(d) An electronic mail service provider shall not be required to create a policy prohibiting or restricting the use of its equipment for the initiation or delivery of unsolicited electronic mail advertisements.

(e) Nothing in this section shall be construed to limit or restrict the rights of an electronic mail service provider under Section 230(c)(1) of Title 47 of the United States Code, or any decision of an electronic mail service provider to permit or to restrict access to or use of its system, or any exercise of its editorial function.

(f) (1) In addition to any other action available under law, any electronic mail service provider whose policy on unsolicited electronic mail advertisements is violated as provided in this section may bring a civil action to recover the actual monetary loss suffered by that provider by reason of that violation, or liquidated damages of fifty dollars ($50) for each electronic mail message initiated or delivered in violation of this section, up to a maximum of twenty-five thousand dollars ($25,000) per day, whichever amount is greater.

(2) In any action brought pursuant to paragraph (1), the court may award reasonable attorney's fees to a prevailing party.

(3) (A) In any action brought pursuant to paragraph (1), the electronic mail service provider shall be required to establish as an element of its cause of action that prior to the alleged violation, the defendant had actual notice of both of the following:

(i) The electronic mail service provider's policy on unsolicited electronic mail advertising.

(ii) The fact that the defendant's unsolicited electronic mail advertisements would use or cause to be used the electronic mail service provider's equipment located in this state.

(B) In this regard, the Legislature finds that with rapid advances in Internet technology, and electronic mail technology in particular, Internet service providers are already experimenting with embedding policy statements directly into the software running on the computers used to provide electronic mail services in a manner that displays the policy statements every time an electronic mail delivery is requested. While the state of the technology does not support such a finding at present, the Legislature believes that, in a given case at some future date, a showing that notice was supplied via electronic means between the sending and receiving computers could be held to constitute actual notice to the sender for purposes of this paragraph.

(4) A violation of this section shall not be subject to Section 17534.

CALIFORNIA PENAL CODE
SECTION 502
(including 2000 amendments)

§ 502. Computer crimes

(a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.

The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data.

(b) For the purposes of this section, the following terms have the following meanings:

(1) "Access" means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

(2) "Computer network" means any system that provides communications between one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication facilities.

(3) "Computer program or software" means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.

(4) "Computer services" includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network.

(5) "Computer system" means a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

(6) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.

(7) "Supporting documentation" includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software.

(8) "Injury" means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or the denial of access to legitimate users of a computer system, network, or program.

(9) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access.

(10) "Computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

(11) "Internet domain name" means a globally unique, hierarchical reference to an Internet host or service, assigned through centralized Internet naming authorities, comprising a series of character strings separated by periods, with the rightmost character string specifying the top of the hierarchy.

(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

(d)(1) Any person who violates any of the provisions of paragraph (1), (2), (4), or (5) of subdivision (c) is punishable by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(2) Any person who violates paragraph (3) of subdivision (c) is punishable as follows:

(A) For the first violation that does not result in injury, and where the value of the computer services used does not exceed four hundred dollars ($400), by a fine not

exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000) or in an injury, or if the value of the computer services used exceeds four hundred dollars ($400), or for any second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(3) Any person who violates paragraph (6) or (7) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding one thousand dollars ($1,000).

(B) For any violation that results in a victim expenditure in an amount not greater than five thousand dollars ($5,000), or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(C) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000), by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(4) Any person who violates paragraph (8) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, a misdemeanor punishable by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in a county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment.

(5) Any person who violates paragraph (9) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not one thousand dollars.

(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(e)(1) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. For the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor, pursuant to the provisions of Section 1714.1 of the Civil Code.

(2) In any action brought pursuant to this subdivision the court may award reasonable attorney's fees.

(3) A community college, state university, or academic institution accredited in this state is required to include computer-related crimes as a specific violation of college or university student conduct policies and regulations that may subject a student to disciplinary sanctions up to and including dismissal from the academic institution. This paragraph shall not apply to the University of California unless the Board of Regents adopts a resolution to that effect.

(4) In any action brought pursuant to this subdivision for a willful violation of the provisions of subdivision (c), where it is proved by clear and convincing evidence that a defendant has been guilty of oppression, fraud, or malice as defined in subdivision (c) of Section 3294 of the Civil Code, the court may additionally award punitive or exemplary damages.

(5) No action may be brought pursuant to this subdivision unless it is initiated within three years of the date of the act complained of, or the date of the discovery of the damage, whichever is later.

(f) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction, nor shall it make illegal any employee labor relations activities that are within the scope and protection of state or federal labor laws.

(g) Any computer, computer system, computer network, or any software or data, owned by the defendant, that is used during the commission of any public offense described in subdivision (c) or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of subdivision (c) shall be subject to forfeiture, as specified in Section 502.01.

(h)(1) Subdivision (c) does not apply to punish any acts which are committed by a person within the scope of his or her lawful employment. For purposes of this section, a person acts within the scope of his or her employment when he or she performs acts which are reasonably necessary to the performance of his or her work assignment.

(2) Paragraph (3) of subdivision (c) does not apply to penalize any acts committed by a person acting outside of his or her lawful employment, provided that the employee's activities do not cause an injury, as defined in paragraph (8) of subdivision (b), to the employer or another, or provided that the value of supplies or computer services, as defined in paragraph (4) of subdivision (b), which are used does not exceed an accumulated total of one hundred dollars ($100).

(i) No activity exempted from prosecution under paragraph (2) of subdivision (h) which incidentally violates paragraph (2), (4), or (7) of subdivision (c) shall be prosecuted under those paragraphs.

(j) For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.

(k) In determining the terms and conditions applicable to a person convicted of a violation of this section the court shall consider the following:

(1) The court shall consider prohibitions on access to and use of computers.

(2) Except as otherwise required by law, the court shall consider alternate sentencing, including community service, if the defendant shows remorse and recognition of the wrongdoing, and an inclination not to repeat the offense.

BILL NUMBER: SB 1386 CHAPTERED
BILL TEXT

CHAPTER 915
FILED WITH SECRETARY OF STATE SEPTEMBER 26, 2002
APPROVED BY GOVERNOR SEPTEMBER 25, 2002
PASSED THE SENATE AUGUST 30, 2002
PASSED THE ASSEMBLY AUGUST 26, 2002
AMENDED IN ASSEMBLY AUGUST 23, 2002
AMENDED IN ASSEMBLY AUGUST 5, 2002
AMENDED IN ASSEMBLY JULY 25, 2002
AMENDED IN ASSEMBLY JUNE 30, 2002
AMENDED IN ASSEMBLY JUNE 20, 2002
AMENDED IN ASSEMBLY JUNE 6, 2002
AMENDED IN SENATE MARCH 20, 2002

INTRODUCED BY Senator Peace
(Principal coauthor: Assembly Member Simitian)

FEBRUARY 12, 2002

An act to amend, renumber, and add Section 1798.82 of, and to add Section 1798.29 to, the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 1386, Peace. Personal information: privacy.

Existing law regulates the maintenance and dissemination of personal information by state agencies, as defined, and requires each agency to keep an accurate account of disclosures made pursuant to specified provisions. Existing law also requires a business, as defined, to take all reasonable steps to destroy a customer's records that contain personal information when the business will no longer retain those records. Existing law provides civil remedies for violations of these provisions.

This bill, operative July 1, 2003, would require a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The bill would permit the notifications required by its provisions to be delayed if a law enforcement agency determines that it would impede a criminal investigation. The bill would require an agency, person, or business that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any breach of security of the data, as specified. The bill would state the intent of the Legislature to preempt all local regulation of the subject matter of the bill. This bill would also make a statement of legislative findings and declarations regarding privacy and financial security.

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1. (a) The privacy and financial security of individuals is increasingly at risk due to the ever more widespread collection of personal information by both the private and public sector.

(b) Credit card transactions, magazine subscriptions, telephone numbers, real estate records, automobile registrations, consumer surveys, warranty registrations, credit reports, and Internet Web sites are all sources of personal information and form the source material for identity thieves.

(c) Identity theft is one of the fastest growing crimes committed in California. Criminals who steal personal information such as social security numbers use the information to open credit card accounts, write bad checks, buy cars, and commit other financial crimes with other people's identities. The Los Angeles County Sheriff's Department reports that the 1,932 identity theft cases it received in the year 2000 represented a 108 percent increase over the previous year's caseload.

(d) Identity theft is costly to the marketplace and to consumers.

(e) According to the Attorney General, victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative.

SEC. 2. Section 1798.29 is added to the Civil Code, to read:

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized aquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the

name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

SEC. 3. Section 1798.82 of the Civil Code is amended and renumbered to read:

1798.84. (a) Any customer injured by a violation of this title may institute a civil action to recover damages.

(b) Any business that violates, proposes to violate, or has violated this title may be enjoined.

(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

SEC. 4. Section 1798.82 is added to the Civil Code, to read:

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in

accordance with its policies in the event of a breach of security of the system.

SEC. 5. This act shall become operative on July 1, 2003.

SEC. 6. This act deals with subject matter that is of statewide concern, and it is the intent of the Legislature that this act supersede and preempt all rules, regulations, codes, statutes, or ordinances or all cities, counties, cities and counties, municipalities, and other local agencies regarding the matters expressly set forth in this act.

UNITED STATES DISTRICT COURT
DISTRICT OF COLUMBIA

FEDERAL TRADE COMMISSION, 600 Pennsylvania Ave., N.W. Washington, DC 20580, Plaintiff,

v.

REVERSEAUCTION.COM, INC., 2401 Pennsylvania Ave, N.W., Suite 300 Washington, DC 20037, a Delaware corporation, Defendant.

CIVIL ACTION NO.

STIPULATED CONSENT AGREEMENT AND FINAL ORDER

On January ___, 2000, plaintiff Federal Trade Commission ("Commission" or "FTC") commenced this action by filing its complaint against defendants ReverseAuction.com, Inc. ("ReverseAuction"). The complaint alleges that the defendant engaged in unfair or deceptive acts or practices in violation of Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, and seeks a permanent injunction and other equitable relief pursuant to Section 13(b) of the FTC Act, 15 U.S.C. § 53(b).

The Commission and defendant ReverseAuction have agreed to the settlement of this action upon the following terms and conditions, without adjudication of any issues of fact or law.

NOW, THEREFORE, the Commission and defendant ReverseAuction, having requested the Court to enter this Order, it is therefore Ordered, Adjudged, and Decreed as follows:

FINDINGS

1. This Court has jurisdiction over the subject matter of this case and has jurisdiction over defendant. Venue in this district is proper;

2. The Commission has the authority under Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), to seek the relief it has requested;

3. The Complaint states a claim upon which injunctive relief may be granted against defendant under Sections 5(a) and 13(b) of the FTC Act, 15 U.S.C. § § 45(a) and 53(b);

4. The activities of the defendant are in or affecting commerce, as defined in Section 4 of the FTC Act, 15 U.S.C. § 44;

5. Defendant has agreed to waive all rights to seek judicial review or otherwise challenge or contest the validity of the Final Order, and defendant waives any right that may arise under the Equal Access to Justice Act, 28 U.S.C.§ 2412;

6. This agreement is for settlement purposes only and does not constitute an admission by defendant that the law has been violated as alleged in the complaint or that the facts as alleged in the complaint, other than the jurisdictional facts, are true.

7. Except as herein provided, this action and the relief awarded herein are in addition to, and not in lieu of, other remedies as may be provided by law; and

8. Entry of the Final Order is in the public interest.

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. "Clear(ly) and prominent(ly)" shall mean in a type size and location that are not obscured by any distracting elements and are sufficiently noticeable for an ordinary consumer to read and comprehend, and in a typeface that contrasts with the background against which it appears.

2. Unless otherwise specified, "Defendant" shall mean ReverseAuction, and each of its successors and assigns, officers, agents, representatives, and employees.

3. "Disclosure" or "disclosed to third party(ies)" shall mean (a) the release of information in personally identifiable form to any other individual, firm, or organization for any purpose or

(b) making publicly available such information by any means including, but not limited to, public posting on or through home pages, e-mail services, message boards, or chat rooms.

4. "Personal identifying information" shall include, but is not limited to, first and last name, home or other physical address (e.g., school), e-mail address, telephone number, social security number, user identification name ("user ID"), feedback rating, or any information that identifies a specific individual, or any information which, when tied to the above, becomes identifiable to a specific individual.

PROHIBITION AGAINST MISREPRESENTATIONS

I.

IT IS HEREBY ORDERED that defendant, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, promotion, or offering of any Internet auction company or web site in or affecting commerce, shall not make any misrepresentation, in any manner, expressly or by implication, about its agreement to comply with or be bound by any company's user agreement, privacy policy, or contract provision, that limits or prohibits the collection, use, or disclosure of consumers' personal identifying information.

II.

IT IS HEREBY ORDERED that defendant, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, promotion, or offering of any Internet auction company or web site in or affecting commerce, shall not make any misrepresentation, in any manner, expressly or by implication, concerning the features, terms, conditions, business practices or privacy policy of any other company, including, but not limited to, the following:

A. Falsely representing that the user ID utilized by consumers on any other Internet company or web site has expired or will expire;

B. Falsely representing that any Internet company or web site directly or indirectly provided ReverseAuction with the personal identifying information of such company's registered users;

C. Falsely representing that any Internet company or web site knew of, or authorized, ReverseAuction's dissemination of unsolicited commercial e-mail to the registered users of such company.

NOTICE REQUIREMENTS

III.

IT IS FURTHER ORDERED that, within five (5) business days of the date of entry of this final order, defendant shall send to all consumers who registered with ReverseAuction as a result of receiving the unsolicited commercial e-mail sent by ReverseAuction to eBay users between November 12, 1999 and November 15, 1999 the following e-mail message:

"ReverseAuction.com is sending this notice as a result of a Settlement Agreement with the Federal Trade Commission.

Between November 12, 1999 and November 15, 1999, you received an unsolicited commercial e-mail message from ReverseAuction.com stating that the user ID you use on eBay "will EXPIRE soon." Our intent was to inform you that we had reserved your eBay ID, for you to use on ReverseAuction.com, if you wished. We did not intend to suggest that the user IDs used by eBay registered users on eBay were about to expire on eBay. eBay did not have any knowledge that ReverseAuction.com had obtained your e-mail address and eBay user ID, nor did eBay give ReverseAuction.com permission to do so. ReverseAuction.com was solely responsible for the dissemination of this e-mail, and regrets any confusion it may have caused among eBay registered users.

ReverseAuction.com has agreed to delete from its database and not otherwise use or disclose the user ID, e-mail address, and feedback rating (which we also

> obtained) of all eBay users who received the e-mail but have not registered with ReverseAuction.com. ReverseAuction.com customers who registered after receiving the e-mail can always cancel their registration at any time and have their information deleted from our database. Please send us a reply e-mail message if you would like to cancel your registration with us. Unless you cancel, your current registration will remain in effect. ReverseAuction.com reaffirms that no other personally identifying information (such as your name, address, telephone number or any other confidential data) was viewed, transmitted, collected or utilized by ReverseAuction.com.
>
> The ReverseAuction.com Privacy Policy, which is posted on our web site, will continue to govern our use of personal identifying information of any registered user on ReverseAuction.com."

Provided that, for any consumer covered by this Section who requested not to receive e-mail or regular mail communications from ReverseAuction under ReverseAuction's Privacy Policy, ReverseAuction, in lieu of sending an e-mail, shall provide the above-referenced message, for a six (6) month period, by causing it to automatically appear on the screen, clearly and prominently, the first time the consumer logs onto the "My Profile" area of the web site.

IV.

IT IS FURTHER ORDERED that within five (5) business days of the date of entry of this final order, defendant shall place on its web site, for a period of six (6) months, a clear and prominent notice that will automatically appear on the screen if and when any eBay registered user who received the e-mail sent by ReverseAuction registers with ReverseAuction:

> "ReverseAuction.com is sending this notice as a result of a Settlement Agreement with the Federal Trade Commission.
>
> Between November 12, 1999 and November 15, 1999, you received an unsolicited commercial e-mail message from ReverseAuction.com stating that the user ID you use on eBay "will EXPIRE soon." Our intent was to inform you that we had reserved your eBay ID, for you to use on ReverseAuction.com, if you wished. We did not intend to suggest that the user IDs used by eBay registered users on eBay were about to expire on eBay. eBay did not have any knowledge that ReverseAuction.com had obtained your e-mail address and eBay user ID, nor did eBay give ReverseAuction.com permission to do so. ReverseAuction.com was solely responsible for the dissemination of this e-mail, and regrets any confusion it may have caused among eBay registered users.
>
> ReverseAuction.com has agreed to delete from its database and not otherwise use or disclose the user ID, e-mail address, and feedback rating (which we also obtained) of all eBay users who received the e-mail but have not registered with

ReverseAuction.com. ReverseAuction.com customers who registered after receiving the e-mail can always cancel their registration at any time and have their information deleted from our database by sending us an e-mail. ReverseAuction.com reaffirms that no other personally identifying information (such as your name, address, telephone number or any other confidential data) was viewed, transmitted, collected or utilized by ReverseAuction.com.

The ReverseAuction.com Privacy Policy, which is posted on our web site, will continue to govern our use of personal identifying information of any registered user on ReverseAuction.com."

REQUIREMENT THAT DEFENDANT DELETE, AND REFRAIN FROM USING OR DISCLOSING, THE USER IDS, E-MAIL ADDRESSES, AND FEEDBACK RATINGS OF CERTAIN EBAY CUSTOMERS

V.

IT IS FURTHER ORDERED that defendant shall delete, and refrain from using or disclosing, the user IDs, e-mail addresses, and feedback ratings of all the eBay registered customers listed below:

A. All eBay customers who received an unsolicited email from ReverseAuction between November 12, 1999 and November 15, 1999, and who have not registered with ReverseAuction.

B. All eBay customers who received an unsolicited e-mail from ReverseAuction between November 12, 1999 and November 15, 1999, who registered with ReverseAuction as a result of such e-mail, and who have elected to cancel their registration with ReverseAuction in response to the notices required under Sections III or IV of this Order.

Provided, however, that defendant may retain the email addresses, user IDs, and/or feedback ratings for so long as needed to fulfill its notice obligation under Sections III and IV, and solely for those purposes, after which such information shall be deleted.

PRIVACY NOTICE

VI.

IT IS FURTHER ORDERED that defendant, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, promotion, or offering of any Internet service or web site, shall provide clear and prominent notice to consumers on the web site of its practices with regard to its collection and use of personal identifying information. Such notice shall include, but is not limited to, disclosure of:

A. what information is being collected (e.g., "name," "home address," "e-mail address," "age," "interests");

B. its intended use(s) and the consumer's ability to control such uses (e.g., the consumer's ability to "opt-in" or "opt-out" of particular uses, such as transfers to third parties);

C. the third parties to whom it will be disclosed (e.g., "advertisers of consumer products," mailing list companies," "the general public");

D. the consumer's ability to obtain access to or directly access such information and the means by which (s)he may do so;

E. the consumer's ability to remove directly or have the information removed from defendants' databases and the means by which (s)he may do so; and

F. the steps defendant has taken to ensure the security of the information collected and/or maintained at the site.

Such notice shall appear on the home page of defendant's Web site(s) and at each location on the site(s) at which such information is collected. Alternatively, defendant may comply with this Section by placing a clear and prominent hyperlink or button labeled PRIVACY NOTICE or PRIVACY POLICY on defendant's home page, and at each location on the site at which personal identifying information is collected, which directly links to the privacy notice screen(s) containing the required information.

DOCUMENT RETENTION

VII.

IT IS FURTHER ORDERED that defendant, and its successors and assigns, shall maintain for at least five (5) years from the date of service of this Order and, upon written request by FTC employees, make available to the FTC for inspection and copying:

A. All records and documents necessary to demonstrate fully its compliance with each provision of this Order, including the notice required by Sections III and IV of this Order;

B . A sample copy of any advertising and promotional material, including e-mail, regarding any Internet auction company or web site operated or maintained by defendant which is disseminated by defendant to any person;

C. Copies of any complaints received by defendant from third parties regarding defendant's promotional or advertising activities.

ORDER DISTRIBUTION

VIII.

IT IS FURTHER ORDERED that, for a period of five (5) years from the date of entry of this Order, defendant, and each of its successors and assigns, shall:

A. Deliver a copy of this Order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities with respect to the subject matter of this Order, and shall secure from each such person a signed and dated statement acknowledging receipt of the Order. Defendant shall deliver this Order to current personnel within thirty (30) days after the date of service of this Order, and to future personnel within thirty (30) days after the person assumes such position or responsibilities; and

B. Maintain for a period of five (5) years after creation, and upon reasonable notice, make available to representatives of the Commission, the original signed and dated acknowledgments of the receipt of copies of the Order, as required by Section VIII(A) of this Order.

COMPLIANCE REPORTING

IX.

IT IS FURTHER ORDERED that, in order that compliance with the provisions of this Order may be monitored:

A. For a period of five (5) years from the date of entry of this Order, defendant, and its successors and assigns, shall notify the Commission of any proposed change in the structure of defendant ReverseAuction that may affect compliance obligations arising under this Order, such as creation, incorporation, dissolution, assignment, sale, or merger of subsidiaries, proposed filing of a bankruptcy petition, or change in the corporate name or address, or other action that would result in the emergence of a successor corporation, thirty (30) days prior to the effective date of any proposed change; *provided*, *however*, that, with respect to any proposed change in the corporation about which defendant learns less than thirty (30) days prior to the date such action is to take place, defendant shall notify the Commission as soon as is practicable after learning of such proposed change;

B. Sixty (60) days after the date of entry of this Order, defendant shall provide a written report to the FTC, sworn to under penalty of perjury, setting forth in detail the manner and form in which the defendant has complied and is complying with this Order;

C. For the purposes of this Order, defendant shall, unless otherwise directed by the Commission's authorized representatives, mail all written notifications to the Commission to:

Associate Director, Division of Financial Practices
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580

Re: FTC v. ReverseAuction.com

RETENTION OF JURISDICTION

X.

IT IS FURTHER ORDERED that the Court retains jurisdiction of this matter for all purposes, including the construction, modification, and enforcement of this Order.

STIPULATED AND AGREED TO BY:

FOR THE PLAINTIFF:

DATED: _____

_____
MICHELLE CHUA
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580
(202) 326-3248 (voice)
(202) 326-2558 (facsimile)

FOR THE DEFENDANT:

DATED: _____

_____ DEBORAH M. LODGE
Patton Boggs, LLP.
2550 M Street, N.W.,
Washington, D.C. 20037

COUNSEL for ReverseAuction.com, Inc.

_____ JOHN MCCARTHY
Chairman of the Board, ReverseAuction.com, Inc.

IT IS SO ORDERED: United States District Judge

Analysis of Proposed Consent Order to Aid Public Comment

Microsoft Corporation, File No. 012 3240

The Federal Trade Commission has accepted, subject to final approval, an agreement containing a consent order from Microsoft Corporation ("Microsoft").

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's proposed order.

Microsoft develops, manufactures, licenses, and supports a myriad of software products, sells hardware devices, provides consulting services, trains and certifies system developers, and offers a variety of online services. This matter concerns allegedly false or misleading representations made in connection with three related Microsoft services: the Passport Single Sign-In service ("Passport"); Passport Express Purchase (generally referred to as "Passport Wallet"); and Kids Passport (referred to collectively as the "Passport services"). Passport is an online authentication service that allows consumers to sign in at multiple Web sites with a single username and password. Passport Wallet and Kids Passport are add-on services that provide online purchasing and parental consent services.

The Commission's proposed complaint alleges that Microsoft misrepresented:

> (1) that it maintained a high level of online security by employing sufficient measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained from or about consumers in connection with the Passport and Passport Wallet services;
>
> (2) that purchases made at a Passport Express Purchase site with Passport Wallet are safer or more secure than purchases made at the same Passport Express Purchase site without using the Passport Wallet;
>
> (3) that Passport did not collect any personally identifiable information other than that described in its privacy policy, when, in fact, Passport collected, and maintained for a limited period of time, a personally identifiable record of the sites to which a Passport user signed in, along with the dates and times of sign in, which customer service representatives linked to a user's name in order to respond to a user's request for service; and
> (4) that the Kids Passport service provided parents with control over the information their children could provide to participating Passport sites and the use of that information by such sites.

The proposed consent order applies to the collection and storage of personal information from or about consumers in connection with the advertising, marketing, promotion, offering for sale, or sale of Passport, Kids Passport, Passport Wallet, any substantially similar product or service, or any multisite online authentication service. It contains provisions designed to prevent Microsoft from engaging in practices similar to those alleged in the complaint in the future.

Specifically, Part I of the proposed order prohibits misrepresentations regarding Microsoft's information practices, including:

- what personal information is collected from or about consumers;
- the extent to which respondent's product or service will maintain, protect or enhance the privacy, confidentiality, or security of any personally identifiable information collected from or about consumers;
- the steps respondent will take with respect to personal information it has collected in the event that it changes the terms of the privacy policy in effect at the time the information was collected;
- the extent to which the service allows parents to control what the information their children can provide to participating sites or the use of that information by such sites; and
- any other matter regarding the collection, use, or disclosure of personally identifiable information.

Part II of the proposed order requires Microsoft to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to Microsoft's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers. Specifically, the order requires Microsoft to:

- designate an employee or employees to coordinate and be accountable for the information security program;
- identify material internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment will include consideration of risks in each area of relevant operation, including: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.
- design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures.
- evaluate and adjust its information security program in light of the results of testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that Microsoft knows or has reason to know may have a material impact on its information security program.

Part III of the proposed order requires that Microsoft obtain within one year, and on a biannual basis thereafter, an assessment and report from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession, certifying that: (1) Microsoft has in place a security program that provides protections that meet or exceed the protections required by Part II of this order; and (2) Microsoft's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumer's personal information has been protected.

Parts IV through VII of the proposed order are reporting and compliance provisions. Part IV requires Microsoft's retention of materials relating to its privacy and security representations and to its compliance with the order's information security program. Part V requires dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part VI ensures notification to the FTC of changes in corporate status. Part VII mandates compliance reports within sixty (60) days after service of the order and at such other times as the Federal Trade Commission may require. Part VII is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the agreement and proposed order or to modify their terms in any way.

Analysis of Proposed Consent Order to Aid Public Comment

Guess?, Inc. and Guess.com, inc., File No. 0223260

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from Guess?, Inc. and Guess.com, inc. ("Guess").

The consent agreement has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's proposed order.

Guess is an international company that designs and produces men's, women's, and children's clothing and accessory products. The company's products are marketed, distributed, and sold under various Guess brand names through its own stores, a limited number of independent retailers, and, its online store at www.guess.com. This matter concerns alleged false or misleading representations Guess made to consumers about the security of personal information collected online through www.guess.com, Guess' online store

The Commission's proposed complaint alleges that Guess misrepresented that the personal information it obtained from consumers through www.guess.com was stored in an unreadable, encrypted format at all times. The complaint alleges that this representation was false because a commonly known attack could and was used to gain access in clear readable text to sensitive personal information, including credit card numbers, that Guess obtained from consumers.

The proposed complaint also alleges that Guess represented that it implemented reasonable and appropriate measures to protect the personal information it obtained from consumers through www.guess.com against loss, misuse, or alteration. The complaint alleges this representation was false because Guess did not employ appropriate measures to detect reasonably foreseeable vulnerabilities and prevent their exploitation.

The proposed order applies to Guess' collection and storage of personal information from or about consumers in connection with its online business. It contains provisions designed to prevent Guess from engaging in practices similar to those alleged in the complaint in the future.

Specifically, Part I of the proposed order prohibits Guess, in connection with the online advertising, marketing, promotion, offering for sale, or sale of any product or service, from misrepresenting the extent to which it maintains and protects the security, confidentiality, or integrity of any personal information collected from or about consumers.

Part II of the proposed order requires Guess to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to Guess's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers. Specifically, the order requires Guess to:

- Designate an employee or employees to coordinate and be accountable for the information security program;
- Identify material internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in

place to control these risks. At a minimum, this risk assessment must include consideration of risks in each area of relevant operation.

- Design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures.
- Evaluate and adjust its information security program in light of the results of testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that Guess knows or has reason to know may have a material impact on its information security program.

Part III of the proposed order requires that Guess obtain within one year, and on a biannual basis thereafter, an assessment and report from a qualified, objective, independent third-party professional, certifying that: (1) Guess has in place a security program that provides protections that meet or exceed the protections required by Part II of this order; and (2) Guess's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumer's personal information has been protected.

Parts IV through VII of the proposed order are reporting and compliance provisions. Part IV requires Guess's to retain documents relating to compliance. For most records, the order requires that the documents be retained for a five-year period. For the assessments and supporting documents, Guess must retain the documents for three years after the date that each assessment is prepared. Part V requires dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part VI ensures notification to the FTC of changes in corporate status. Part VII mandates that Guess submit compliance reports to the FTC. Part VIII is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed order or to modify their terms in any way.

VIRGINIA CODE
TITLE 8.01. CIVIL REMEDIES AND PROCEDURE
CHAPTER 9. PERSONAL JURISDICTION IN CERTAIN ACTIONS
SECTION 8.01-328.1 (2003)

§ 8.01-328.1. When personal jurisdiction over person may be exercised.

A. A court may exercise personal jurisdiction over a person, who acts directly or by an agent, as to a cause of action arising from the person's:

1. Transacting any business in this Commonwealth;
2. Contracting to supply services or things in this Commonwealth;
3. Causing tortious injury by an act or omission in this Commonwealth;
4. Causing tortious injury in this Commonwealth by an act or omission outside this Commonwealth if he regularly does or solicits business, or engages in any other persistent course of conduct, or derives substantial revenue from goods used or consumed or services rendered, in this Commonwealth;
5. Causing injury in this Commonwealth to any person by breach of warranty expressly or impliedly made in the sale of goods outside this Commonwealth when he might reasonably have expected such person to use, consume, or be affected by the goods in this Commonwealth, provided that he also regularly does or solicits business, or engages in any other persistent course of conduct, or derives substantial revenue from goods used or consumed or services rendered in this Commonwealth;
6. Having an interest in, using, or possessing real property in this Commonwealth;
7. Contracting to insure any person, property, or risk located within this Commonwealth at the time of contracting;
8. Having (i) executed an agreement in this Commonwealth which obligates the person to pay spousal support or child support to a domiciliary of this Commonwealth, or to a person who has satisfied the residency requirements in suits for annulments or divorce for members of the armed forces pursuant to § 20-97 provided proof of service of process on a nonresident party is made by a law-enforcement officer or other person authorized to serve process in the jurisdiction where the nonresident party is located, (ii) been ordered to pay spousal support or child support pursuant to an order entered by any court of competent jurisdiction in this Commonwealth having in personam jurisdiction over such person, or (iii) shown by personal conduct in this Commonwealth, as alleged by affidavit, that the person conceived or fathered a child in this Commonwealth;
9. Having maintained within this Commonwealth a matrimonial domicile at the time of separation of the parties upon which grounds for divorce or separate maintenance is based, or at the time a cause of action arose for divorce or separate maintenance or at the time of commencement of such suit, if the other party to the matrimonial relationship resides herein; or
10. Having incurred a tangible personal property tax liability to any political subdivision of the Commonwealth.

Jurisdiction in subdivision 9 is valid only upon proof of service of process pursuant to § 8.01-296 on the nonresident party by a person authorized under the provisions of § 8.01-320. Jurisdiction under subdivision 8 (iii) of this subsection is valid only upon proof of personal service on a nonresident pursuant to § 8.01-320.

B. Using a computer or computer network located in the Commonwealth shall constitute an act in the Commonwealth. For purposes of this subsection, "use" and "computer network" shall have the same meanings as those contained in § 18.2-152.2.

C. When jurisdiction over a person is based solely upon this section, only a cause of action arising from acts enumerated in this section may be asserted against him; however, nothing contained in this chapter shall limit, restrict or otherwise affect the jurisdiction of any court of this Commonwealth over foreign corporations which are subject to service of process pursuant to the provisions of any other statute.

VIRGINIA CODE
TITLE 18.2. CRIMES AND OFFENSES GENERALLY
CHAPTER 5. CRIMES AGAINST PROPERTY
ARTICLE 7.1. COMPUTER CRIMES
SECTIONS 18.2-152.2, 152.3:1, 152.4, 152.12 & 152.16 (2003)
(including amendments by Acts 2003, ch. 987 & 1016, approved April 3, 2003)

§ 18.2-152.2. Definitions.

For purposes of this article:

"Computer" means an electronic, magnetic, optical, hydraulic or organic device or group of devices which, pursuant to a computer program, to human instruction, or to permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. The term "computer" includes any connected or directly related device, equipment, or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device.

"Computer data" means any representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared and is intended to be processed, is being processed, or has been processed in a computer or computer network. "Computer data" may be in any form, whether readable only by a computer or only by a human or by either, including, but not limited to, computer printouts, magnetic storage media, punched cards, or stored internally in the memory of the computer.

"Computer network" means two or more computers connected by a network.

"Computer operation" means arithmetic, logical, monitoring, storage or retrieval functions and any combination thereof, and includes, but is not limited to, communication with, storage of data to, or retrieval of data from any device or human hand manipulation of electronic or magnetic impulses. A "computer operation" for a particular computer may also be any function for which that computer was generally designed.

"Computer program" means an ordered set of data representing coded instructions or statements that, when executed by a computer, causes the computer to perform one or more computer operations.

"Computer services" means computer time or services, including data processing services, Internet services, electronic mail services, electronic message services, or information or data stored in connection therewith.

"Computer software" means a set of computer programs, procedures and associated documentation concerned with computer data or with the operation of a computer, computer program, or computer network.

"Electronic mail service provider" means any person who (i) is an intermediary in sending or receiving electronic mail and (ii) provides to end-users of electronic mail services the ability to send or receive electronic mail.

"Financial instrument" includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computerized representation thereof.

"Network" means any combination of digital transmission facilities and packet switches, routers, and similar equipment interconnected to enable the exchange of computer data.

"Owner" means an owner or lessee of a computer or a computer network or an owner, lessee, or licensee of computer data, computer programs, or computer software.

"Person" shall include any individual, partnership, association, corporation or joint venture.

"Property" shall include:

1. Real property;
2. Computers and computer networks;
3. Financial instruments, computer data, computer programs, computer software and all other personal property regardless of whether they are:

a. Tangible or intangible;
b. In a format readable by humans or by a computer;
c. In transit between computers or within a computer network or between any devices which comprise a computer; or
d. Located on any paper or in any device on which it is stored by a computer or by a human; and
4. Computer services.

A person "uses" a computer or computer network when he attempts to cause or causes:

1. A computer or computer network to perform or to stop performing computer operations;
2. The withholding or denial of the use of a computer, computer network, computer program, computer data or computer software to another user; or
3. A person to put false information into a computer.

A person is "without authority" when he has no right or permission of the owner to use a computer or he uses a computer or computer network in a manner exceeding such right or permission.

§ 18.2-152.3:1. Transmission of unsolicited bulk electronic mail; penalty.

A. Any person who:

1. Uses a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers; or

2. Knowingly sells, gives, or otherwise distributes or possesses with the intent to sell, give, or distribute software that (i) is primarily designed or produced for the purpose of facilitating or enabling the falsification of electronic mail transmission information or other routing information; (ii) has only limited commercially significant purpose or use other than to facilitate or enable the falsification of electronic mail transmission information or other routing information; or (iii) is marketed by that person acting alone or with another for use in facilitating or enabling the falsification of electronic mail transmission information or other routing information is guilty of a Class 1 misdemeanor.

B. A person is guilty of a Class 6 felony if he commits a violation of subsection A and:

1. The volume of UBE transmitted exceeded 10,000 attempted recipients in any 24-hour period, 100,000 attempted recipients in any 30-day time period, or one million attempted recipients in any one-year time period; or

2. The revenue generated from a specific UBE transmission exceeded $1,000 or the total revenue generated from all UBE transmitted to any EMSP exceeded $50,000.

C. A person is guilty of a Class 6 felony if he knowingly hires, employs, uses, or permits any minor to assist in the transmission of UBE in violation of subdivision B 1 or subdivision B 2.

§ 18.2-152.4. Computer trespass; penalty.

A. It shall be unlawful for any person to use a computer or computer network without authority and with the intent to:

1. Temporarily or permanently remove, halt, or otherwise disable any computer data, computer programs, or computer software from a computer or computer network;
2. Cause a computer to malfunction, regardless of how long the malfunction persists;
3. Alter or erase any computer data, computer programs, or computer software;
4. Effect the creation or alteration of a financial instrument or of an electronic transfer of funds;
5. Cause physical injury to the property of another;
6. Make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network.

B. Any person who violates this section shall be guilty of computer trespass, which offense shall be punishable as a Class 1 misdemeanor. If there is damage to the property of another valued at $2,500 or more caused by such person's malicious act in violation of this section, the offense shall be punishable as a Class 6 felony.

C. Nothing in this section shall be construed to interfere with or prohibit terms or conditions in a contract or license related to computers, computer data, computer networks, computer operations, computer programs, computer services, or computer software or to create any liability by reason of terms or conditions adopted by, or technical measures implemented by, a Virginia-based electronic mail service provider to prevent the transmission of unsolicited electronic mail in violation of this article. Nothing in this section shall be construed to prohibit the monitoring of computer usage of, the otherwise lawful copying of data of, or the denial of computer or Internet access to a minor by a parent or legal guardian of the minor.

§ 18.2-152.12. Civil relief; damages.

A. Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained, and the costs of suit. Without limiting the generality of the term, "damages" shall include loss of profits.

B. If the injury under this article arises from the transmission of unsolicited bulk electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider where the defendant has knowledge of the authority or policies of the EMSP or where the authority or policies of the EMSP are available on the electronic mail service provider's website, the injured person, other than an electronic mail service provider, may also recover attorneys' fees and costs, and may elect, in lieu of actual damages, to recover the lesser of $10 for each and every unsolicited bulk electronic mail message transmitted in violation of this article, or $25,000 per day. The injured person shall not have a cause of action against the electronic mail service provider that merely transmits the unsolicited bulk electronic mail over its computer network. Transmission of electronic mail from an organization to its members shall not be deemed to be unsolicited bulk electronic mail.

C. If the injury under this article arises from the transmission of unsolicited bulk electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider where the defendant has knowledge of the authority or policies of the EMSP or where the authority or policies of the EMSP are available on the electronic mail service provider's website, an injured electronic mail service provider may also recover attorneys' fees and costs, and may elect, in lieu of actual damages, to recover $1 for each and every intended recipient of an unsolicited bulk electronic mail message where the intended recipient is an end user of the EMSP or $25,000 for each day an attempt is made to transmit an unsolicited bulk electronic mail message to an end user of the EMSP. In calculating the statutory damages under this provision, the court may adjust the amount awarded as necessary, but in doing so shall take into account the number of complaints to the EMSP generated by the defendant's messages, the defendant's degree of culpability, the defendant's prior history of such conduct, and the extent of economic gain resulting from the conduct. Transmission of electronic mail from an organization to its members shall not be deemed to be unsolicited bulk electronic mail.

D. At the request of any party to an action brought pursuant to this section, the court may, in its discretion, conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer network, computer data, computer program and computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party and in such a way as to protect the privacy of nonparties who complain about violations of this section.

E. The provisions of this article shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

F. A civil action under this section must be commenced before expiration of the time period prescribed in § 8.01-40.1. In actions alleging injury arising from the transmission of unsolicited bulk electronic mail, personal jurisdiction may be exercised pursuant to § 8.01-328.1.

§ 18.2-152.16. Forfeitures for violation of this article.

All moneys and other income, including all proceeds earned but not yet received by a defendant from a third party as a result of the defendant's violations of this article, and all computer equipment, all computer software, and all personal property used in connection with any violation of this article known by the owner thereof to have been used in violation of this article, shall be subject to lawful seizure by a law-enforcement officer and forfeiture by the Commonwealth in accordance with the procedures set forth in Chapter 22.1 (§ 19.2-386.1 et seq.) of Title 19.2, applied mutatis mutandis.

ACCA Conference
2003

Scott Shipman, Head Privacy Guru, eBay Inc.

Agenda

- What is eBay?
- Privacy, the eBay way.
- Privacy Issues

What is eBay

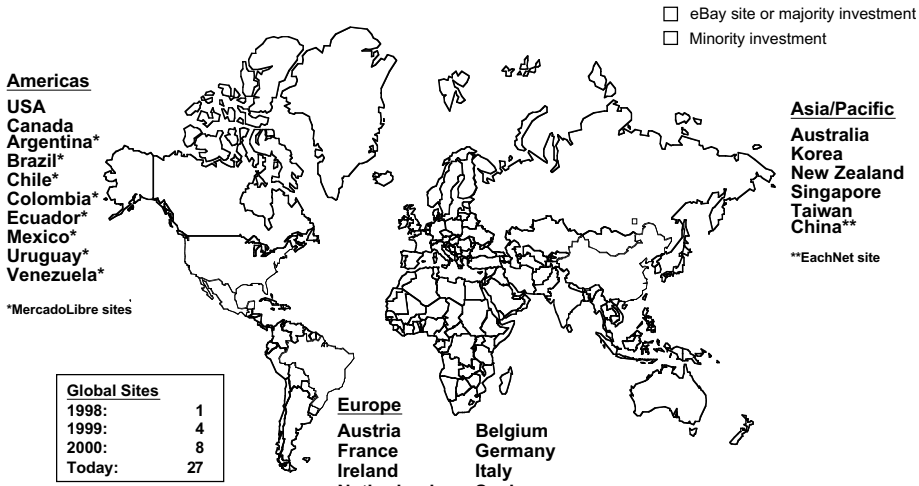
What is eBay

The world's online marketplace

eBay's Vision

Provide a global online trading platform where practically anyone can trade practically anything

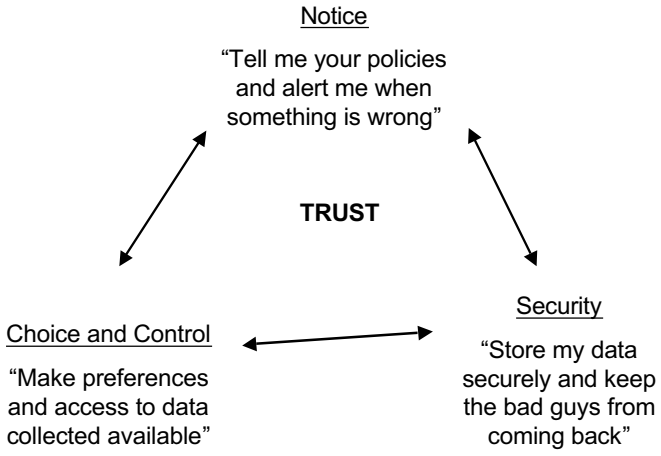
eBay is a Global Company



Privacy Vision

- Provide an open environment that facilitates online trade through trust
- Trust is facilitated by the fair information principles, and by providing our users with:
  - notice and communication
  - choice and control
  - security, authentication and enforcement
- Trust is earned with integrity and time

Privacy the eBay Way



Privacy the eBay Way

Privacy Central

You've come to the right place if you want to learn more about eBay's Privacy Policy and how we protect your privacy. Find out how you can help protect your online privacy and what you can do when something goes wrong.

It is our goal to make our privacy practices easy to understand. We have created easy-to-read summaries, privacy principles, a privacy chart, and continue to implement privacy enhancing technology to help summarize our full privacy policy. If you have questions about any part of this summary or if you would like more detailed information, we encourage you to review our full Privacy Policy

Our core privacy principles

Our core privacy principles remain the same throughout eBay worldwide:

1. We will not sell or rent your information to third parties for marketing purposes and will only disclose your information in accordance with our Privacy Policy and/or with your permission.
2. We do share your information with third parties to help provide our services, to allow members to contact you, to enforce our terms and conditions, and to help keep our community safe.
3. Your information will be shared with third parties for services or features on eBay that you have chosen (such as insurance, escrow, dispute resolution) only when absolutely necessary and under confidential restrictions.
4. Third parties are not permitted to sell the information we provide to them or to disclose it in any other way without your consent.
5. We give you choices about how you wish to be contacted by eBay.
6. We use safe, secure technology and other privacy protection programs to keep your information secure on eBay.
7. We will provide you with notice if our privacy policy changes and an opportunity to reject such changes.
8. We let you change your information so that you can keep it up to date.
9. Other eBay companies that have access to your information in accordance with the policy are required to protect your information at least as strictly as we do.

Privacy the eBay Way

Appendix to the Privacy Policy

How third parties may have access to your information you disclose to eBay.

Below is an easy to read chart that describes the ways in which we use your information and allow others to use your information. It's important to remember that eBay will not sell or rent your information to third parties for marketing purposes, and will only disclose your information in accordance with our Privacy Policy and/or with your permission. As you will read, personally identifiable information is for the most part only shared with third parties in order to complete a transaction or an activity you have initiated on our site. Additionally, you will see that we do not share your personally identifiable information with advertisers. While we do share contact information and other public information that is available on the site with law enforcement to help keep the community a safe place to trade, we do not provide financial, historical, billing, or other non-public information to law enforcement unless required to do so by law.

It is our goal to make our privacy practices easy to understand. We have created easy-to-read summaries, privacy principles, a privacy chart, and we are working on privacy-enhancing technology to help summarize our full privacy policy. If you have questions about any part of this summary or if you would like more detailed information, we encourage you to review our full Privacy Policy

Personal Information	Advertisers	Internal Service Providers	External Service Providers	eBay Community	Legal Requests
Full Name		2	3	4	5
User ID		2	3	5	5
Email Address		2	3	4*	5
Street Address		2	3		5
State	1	2	3	4	5
City	1	2	3	4	5
Zip Code	1	2	3	4	5
Phone Number		2	3	4	5
Country	1	2	3	4	5

Privacy Issues

- Spam Laws
- Privacy Laws
- Regulatory Enforcement

Privacy Issues

- Spam Laws
  - Identification of source
  - Content labeling
  - Opt-in and Opt-out
  - Criminal and Civil penalties

Privacy Issues

- Privacy Laws
  - Primary v. Secondary Uses
  - Opt-in v. Opt-out
  - Notifications for breach
  - Affiliate v. non-affiliate sharing

Privacy Issues

- Enforcement
  - Recent FTC actions
  - Lawsuits
  - Criminal liability

Privacy Hypothetical

European/Cross-border Considerations

1. In connection with the acquisition of Big Ben, American's due diligence should have examined the level of compliance by Big Ben and each Big Ben subsidiary with local data protection laws. This should have included confirmation that there is a legal basis to process data under the applicable law and that all required filings of data processing activities – consumer, employee and perhaps shareholder - have been made. Additionally, contracts with suppliers, particularly processors outside the EU that are not in adequate countries, should have the necessary data protection safeguards.

2. The migration of all of Big Ben's European consumer data to American's global centralized database in San Francisco involves the transfer of personal data from at least the UK to the US. The facts are not clear as to whether each Big Ben subsidiary throughout Europe keeps its own databases or whether they are all consolidated in the UK. It is critical that this be examined and fully understood because some potential derogations will require approval from national data protection authorities.

   To transfer the consumer database to San Francisco it is necessary to understand what is going to be done with the data. If American is going to act as a mere data processor – that is the data is stored on American servers but not accessed or manipulated by American, a standard EU processor agreement between Big Ben (and perhaps the Big Ben subs) is all that is required. If American is considered a data controller because its activities go beyond mere processing, a derogation is required. The possibilities are:
   - Consent – Big Ben would have to approach each consumer, fully disclose what it proposed to do with the consumer's data, and obtain "unambiguous consent." In most countries, but not all, this can be done by e-mail.
   - Transfer is required for performance of a contract – This narrowly interpreted derogation is probably not applicable in this fact situation.
   - Transfer is required for public interest – Inapplicable.
   - Transfer required to protect vital interests of data subject – Inapplicable.
   - Transfer made from public register – Inapplicable.
   - Safe Harbor – American puts into place all the required safeguards, contracts and audit mechanisms to allow it to certify compliance with the Safe Harbor principles to the US Department of Commerce with respect to the European consumer data.
   - Model Contract – American and Big Ben (and possible all the other Big Ben subs) enter into EU Model Contracts and, where required, obtain necessary approvals from national Data Protection Authorities (which approval cannot be withheld).
   - Ad Hoc Contract – American and Big Ben (and possibly other Big Ben subs) enter into contracts not in keeping with the EU Model Contract and try to obtain approval of relevant Data Protection Authorities. This is a long process and in the end the DPA's are unlikely to approve anything other than Model Contracts.
   - Code of Conduct /Binding Corporate Rules – American adopts a corporate code of conduct in a manner that is binding on all American companies throughout the world (thus likely involving the approval by the appropriate organ of corporate governance in each company). The code includes the basic obligations of the model contract and is enforceable against American and its affiliates by third parties. American must then seek approval of the code from the Data Protection Authority in the UK and each other European country from which the consumer data is being exported.

3. The outsourcing and centralization of American's global HR, payroll and benefits databases to Infrastructure Company Ltd. In Bangalore, India involves the transferring of personal data from at least the US to India and the UK and other countries in which Big Ben has subs to India. Turning first to the US, it is important to understand whether any protected healthcare information under HIPAA is being transferred and maintained in India. If so, the requirement to enter into a Business Associate Agreement may arise. It is also important to understand what employees may have been told with respect to any employee privacy statement that American may have issued and to make certain the described outsourcing is within the terms of that statement. In any event, the outsourcing agreement with Infra for the US personal data should include appropriate personal data handling provisions assuring that Infra will use the data only to provide services to American, will keep the data secure and will not transfer the data to any third party without the permission of American.

   The transfer of employee personal information from the European countries to India, which is not considered by the EU to have "adequate" data protection laws, is more complicated. Since Infra is clearly using the data to make decisions on hiring, firing, promotions and benefits it is clearly a data controller and not just a data processor. Accordingly, American has to identify and put into place one of the derogations described above with respect to its European employee data (note Safe Harbor will not work since that is only applicable to transfers to the US). Additionally, the "picture organization chart program" that Infra is to institute and maintain is an additional level of problem. To transfer "sensitive personal data" data out of Europe it is necessary to have the affirmative consent of the data subject. Any other derogation (or even an "opt-out" consent) is insufficient. Since a picture may reveal race, and potentially other attributes that fall within the category of sensitive personal data, the affirmative consent of the employees of Big Ben and its European subs is required.

HIPPA/GLB Issues and Analysis

Prior to entering the consumer market, American Company must understand the extent to which HIPAA applies to it and its product – the Never Get Sick Again tank.

The first question is whether American is a Covered Entity under HIPAA. A Covered Entity is, inter alia, a health care provider that transmits PHI related to a transaction covered under HIPAA. The regulatory definition of "health care" includes supplies related to the health care of an individual, including preventative care. The manufacture and sale of the NGSA may bring American within the definition of a Covered Entity under HIPAA because "[i]t is claimed that the NGSA will cure all medical illnesses." Nevertheless, American – as a manufacturer of equipment -- does not fall squarely within the definitions of a provider of health care services (as would a doctor or a hospital that provides services rather than a product) so the issue cannot be answered definitively. For purposes of this response, we will assume that American is a HIPAA Covered Entity.

The next question is whether Install Company is a Business Associate under HIPAA – if so, Install Company and American Company must execute a Business Associate Agreement. A Business Associate includes any third party entity that performs services for the Covered Entity and in so doing gains access to and uses PHI. The definition of PHI is information, stored in any medium, that is "created or received by a health care provider" and "relates to the past, present or future" health of the individual. Here, Install does gain access to consumer information – and even access to health information – but that information is provided directly by the consumer to Install (and not by American to Install) and therefore does not likely fall within the definition of PHI. However, if American Company gains health information from the customer and then provides it to Install, then American and Install must enter into a Business Associate agreement. So, the analysis turns on the underlying relationship between Install and American – is Install simply an authorized provider of services directly to the ultimate customer, or a "Business Associate" to American?

Unlike Install Company, Computer Company appears to more squarely fit within the definition of Business Associate. In addition, it is important to note that Computer Company is not itself a Covered Entity since there is no affiliation with American Company. Here, American has retained Computer Company to perform services. Importantly, it is highly likely and probably necessary for Computer Company to gain access to and use PHI in connection with its "build[ing] and maintain[ing] ... the networked servers that store the medical information of consumers...." A Business Associate agreement must be signed (again, this assumes that American is a Covered Entity). The key issues to negotiate are: indemnities, audit rights, and inclusion of a third party beneficiary disclaimer.

GLB potentially applies to the financing aspect of American's business. The first inquiry is whether American or its wholly owned subsidiary Money is a GLB-regulated "financial institution". The definition of financial institution includes any entity that "extends credit". This definition would clearly apply to Money, and also to American because American "controls" its wholly-owned subsidiary Money. So, American is subject to GLB directly by way of the activities of Money – providing financing. Because of the affiliate relationship and direct regulation as financial institutions, no written agreement is necessary between American and Money as Money is not an "nonaffiliated third party" service provider.

Credit Company, however, is a nonaffiliated third party provider of services to Money/American, and obtains and uses NPI in order to provide the services to Money. As such, a written agreement must be signed between Money/American and Credit Company that specifies narrow use only to establish "credit worthiness" for Money/American, and requires Credit Company to install an adequate information security program.

Refi is also a wholly-owned subsidiary of American and therefore is a affiliate – accordingly, no written agreement is needed for American to share the information with Refi. Like Money, Refi is directly subject to GLB and it (or American) must comply with GLB in its capacity as a regulated financial institution.

Finally, Data Server is not an affiliate and therefore is not directly regulated by GLB. It does have access to and uses NPI to "store and arrange all consumer data" at Data Server's home office. Accordingly, Refi/American and Data Server must enter into a written agreement covering the use and disclosure of NPI. The key issues to negotiate are: indemnities, audit rights, and inclusion of a third party beneficiary disclaimer.

California Spam, Privacy, Security and Data Sharing Issues

1. **Spam and Harvesting.** In connection with American's email marketing efforts, American should have conducted a state-by-state analysis of state spam and anti-harvesting laws. Most states have spam laws that define spam as the receipt of an unsolicited email containing an advertisement or commercial message, by a citizen of that state. Additionally, most states do not prevent unsolicited email so long as it:

- does not contain deceptive headers or footers (email addressing),
- provides a method to opt-out (may be statutorily required to provide a 1-800 number and an email link) and/or,
- contains an appropriate label in the subject line (such as ADV:, or ADV: ADLT for adult content).

However, recently California passed a spam law that prevents the sending of an email that contains an "advertisement" unless the recipient has consented to receiving such email. This is an opt-in standard. The law regulates businesses that are located in California as well as anyone who sends to an email address that is regularly accessed by someone in California. There is an exception when there is an existing business relationship or the recipient has initiated an inquiry, but in order to meet the exception, all spam must contain an opt-out. Importantly, the law also penalizes "advertisers" equally as initiators of the email and therefore affiliate or viral email campaigns may subject American to liability here although the facts do not provide us with enough to assess that component. Finally, amongst other causes of action, the California law makes it illegal to harvest email addresses from the Internet or web sites to then initiate spam.

American's summer interns may subject American to liability if they continue to harvest email after the effective date of the California law. While prior acts and emails are not covered, collecting email addresses from the public Internet (the law does not discriminate between consumer and business email addresses and therefore American arguably could not even collect business email addresses for the B-2-B component of their business) for the purpose of sending spam will violate California law. Looking at the message, it merely as to offer the disposition of goods or services to constitute an advertisement under the law. While one could argue that on it's face, the email does not offer to sell anything, it is likely that a court would rule that it does meet the definition of an advertisement.

The penalty for sending spam in California is $1,000 per email up to $1,000,000 per incident. It is unclear what an incident is but it may be related to one event that sends out email of the same message to a group of individuals. American may be able to reduce their liability by creating an internal spam and privacy policy that prevents employees from sending spam. If they can prove that they acted reasonably with respect to that policy, then the penalty can be reduced to a maximum fine of $100 per email up to $100,000 per incident.

2. **Privacy Policy.** It is not clear from the fact pattern whether American has a privacy policy on it's website or on pages where American collects personal information. In order to comply with California law, all California companies that collect personal information online must disclose their privacy practices with respect to the personal information collected. Failure to provide a privacy policy within 30 days once American has been notified is a violation of law.

3. **Security.** American should have a security incident response policy in place to enable them to act quickly in light of the hack on their systems. Under California law, any company that stores personal information about a Californian must disclose to data subject events that are "unauthorized acquisition" to name and one of any of the following pieces of information: social security number, drivers license, credit or financial account with password or pin. If the information is stored in an encrypted state, then no notice to the data subject is required.

American's first response should be to determine whether the information is encrypted as well as to determine what systems were authorized. It does not matter that the access was from an old employee, as they are no longer authorized to access information.

If it turns out that the information was not encrypted completely and American reasonably believes that it was acquired, then it must notify the data subjects. If American does not have a notification policy, it must follow one of the proscribed procedures in the law. If it cannot identify each individual or the number of individuals is large, American may have no choice but to provide notice via newspaper. Other methods are traditional post, phone, email and web site notifications if such notice is reasonably likely to reach the recipient and/or is part of your internal notification policy.

4. **Data Sharing.** American should closely document all of the personal and financial data sharing between affiliates and third parties. While GLBA regulates "financial institutions" it does not restrict sharing between corporate affiliates. However, California has a financial privacy law that does restrict sharing information between affiliates as to unaffiliated third parties. It can be quickly summarized as:

- Third party sharing = opt-in
- Non-Financial Institution Affiliate sharing = opt-out
- Financial Institution non-affiliate sharing = opt-out
- Affiliate Financial Institution sharing = no choice required.

This law restricts the sharing of financial information about Californians and therefore may apply to businesses located outside of California as well as American. An important note on this topic is that the renewal of the Fair Credit Reporting Act "may" preempt the affiliate sharing provisions of the California law, however at this time it does not.

