



Monday, October 1, 2012

2:30 PM - 4:00 PM

**702 – Security Breach! What Should You
Have Done Before? What Should You Do
Now?**

Kerry Childe

Senior Privacy and Regulatory Counsel

TG

Ann Chilton

Global Compliance Officer and Regional Managing Attorney for the US/Canada

Environmental Resources Management, Inc.

Aryeh Friedman

Chief Privacy Officer & Senior Compliance Counsel

Dun & Bradstreet

Bobby Turnage, Jr.

Partner

Venable LLP

Faculty Biographies

Kerry Childe

Kerry Childe is the senior privacy and regulatory counsel at Texas Guaranteed Student Loan Corporation in Round Rock, TX, where she is responsible for TG's privacy program and regulatory compliance in the areas of privacy, security, and the federal student loan program TG administers, and provides general corporate legal advice and counsel, including in areas such as social media, products and trade practice, and operations. She has written and speaks regularly on privacy and security issues.

Prior to joining TG as its privacy and regulatory counsel, Ms. Childe was the associate general counsel for a small publicly-traded company in Texas, providing general corporate advice and counsel and assistance with the corporation's regulatory filings and privacy practices.

She is the secretary for the ACC's IT, Privacy, and E-Commerce Committee, a member of the Small Law Department and Financial Services Committees, and a member of the ACC's Austin Chapter. She is a member of the American Bar Association section of science and technology law, and administrative law and regulatory practice. She is also a member of the Texas Choral Consort.

Ms. Childe received her BA at the University of Nebraska-Lincoln and is a graduate of Baylor Law School.

Ann Chilton

Ann Marley Chilton is the global compliance officer and regional managing attorney for the US/Canada at Environmental Resources Management, Inc. (ERM). ERM is a 4,700 person international environmental firm that provides environmental and sustainability services to Fortune 1000 clients in over 44 countries. Ms. Chilton runs ERM's global compliance function and also leads the US/Canada law team. A key focus of her compliance practice is international anti-bribery/corruption counseling and process improvement pursuant to not only the US Federal Sentencing Guidelines for Organizations, but also international GRI and UN Global Compact standards.

Ms. Chilton previously served in-house with the Motorola and Freescale law departments. For these entities, in addition to her duties related to the IPO, she supervised complex commercial, intellectual property, and insured matters litigation. In private practice with Fulbright & Jaworski in Austin, TX, Ms. Chilton served on the national counsel team for Bayer Corporation. In private practice in Chicago, she was on the national counsel team for certain companies at Lloyd's of London.

Ms. Chilton participates in developing international compliance program standards and is one of the seventeen members of the G4 version working group on anti-corruption reporting standards for GRI. Ms. Chilton also participates in ERM's charity, the ERM Foundation. Recently, Ms. Chilton received Ethisphere Magazine's designation as a Top Compliance and Ethics Officer on the 2011 Attorney-Who-Matter list.

Ms. Chilton is an undergraduate alumni of Rice University and a law alumni of the University of Texas School of Law. Ms. Chilton is also a Certified Compliance and Ethics professional (CCEP).

Aryeh Friedman

Aryeh Friedman is the chief privacy officer and senior compliance counsel at Dun & Bradstreet in Short Hills, NJ. He has global responsibility for privacy and data security, anti-corruption compliance, export and trade sanctions law compliance, record and electronic information management (e-RIM), code of conduct compliance and compliance investigations and ethics training.

Prior to joining Dun & Bradstreet, Mr. Friedman was the chief privacy officer at Pfizer. Mr. Friedman also has an extensive background in antitrust law, serving as chief antitrust counsel at Wyeth and before that BT and AT&T. Prior to going in-house, Mr. Friedman was an associate at Paul, Weiss, Rifkind Wharton & Garrison and Drinker, Biddle & Reath.

Mr. Friedman has taught for many years at the Wharton School of the University of Pennsylvania in the Legal Studies and Business Ethics Department. Mr. Friedman is vice chair of the ABA's Privacy and Information Security Committee, and has written and edited numerous books for the ABA including the Data Security Handbook and the Privacy chapter of Consumer Protection Legal Developments Update. He is also the author of "Legal Ethics for In-House Counsel" (BNA 2012) and was profiled in the January/February 2012 ACC Docket.

Mr. Friedman received a BS from Cornell University and his JD from the New York University School of Law.

Bobby Turnage, Jr.


Bobby Turnage is a partner with Venable's corporate practice group. He focuses his work primarily on helping companies address the numerous legal challenges that arise from doing business on the Web, including counseling on such matters as privacy and data security, intellectual property, domains and cybersquatting, online advertising, litigation management and third-party content. He has nearly 20 years of legal experience in private practice, the military and as in-house counsel.

702 Security Breach! What Should You Have Done Before? What Should You Do Now?

Prior to joining Venable, Mr. Turnage served as senior vice president, general counsel and secretary for Network Solutions, LLC, in Northern Virginia. In addition to prior work as a litigation associate in private practice and as a prosecutor and defense lawyer for the Army Reserve JAG Corps, he also previously served as associate general counsel for VeriSign, Inc. Having worked as both an executive and a lawyer embedded in a business, he brings valuable experience that enables him to provide practical, business-focused legal advice on matters faced by businesses in their daily operations.

Mr. Turnage recently completed a term as chairman of the General Counsel Committee of the Northern Virginia Technology Council. He is a past member of ACC, and a past board member of Home Care Delivered, Inc. Mr. Turnage's military awards include the Meritorious Service Medal, Army Commendation Medal (1OLC), Army Achievement Medal (1OLC), Leatherneck Dress Blues Award (USMC), and Navy League Outstanding Marine Corps Recruit Award (USMC).

Mr. Turnage received a BS in business from Virginia Commonwealth University and is a graduate of the University of Mississippi School of Law.




ACC'S
ANNUAL MEETING
2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT

ANACC.COM

Association of
Corporate Counsel

Security Breach! What Should You Have Done Before? What Should You Do Now?

A Dramatic Presentation



ACC'S
ANNUAL MEETING
2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT


ANACC.COM

Association of
Corporate Counsel

Presenters

- **Kerry Childe**, Senior Privacy and Regulatory Counsel, Texas Guaranteed Student Loan Corporation
- **Ann Chilton**, Global Compliance Officer and Regional Managing Attorney for the US/Canada, Environmental Resources Management, Inc.
- **Aryeh Friedman**, Chief Privacy Officer & Senior Compliance Counsel, Dun & Bradstreet
- **Bobby Turnage, Jr.**, Partner, Venable LLP


ACC'S ANNUAL MEETING 2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT



Acc Association of Corporate Counsel

The opinions presented here represent our individual opinions and are not necessarily those of any employer or ACC. This presentation does not constitute the provision of legal advice, and does not create an attorney-client relationship. You are strongly encouraged to contact your counsel for advice.


ACC'S ANNUAL MEETING 2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT




Acc Association of Corporate Counsel

HEAD IN THE CLOUDS

ACC'S ANNUAL MEETING 2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT



#ACCAM12




AM.ACC.COM




DISCUSSION


ACC'S ANNUAL MEETING 2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT



#ACCAM12







AM.ACC.COM




MONEY NOW!


ACC'S ANNUAL MEETING
2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT



#ACCAM12








AM.ACC.COM




DISCUSSION


ACC'S ANNUAL MEETING
2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT



#ACCAM12




AM.ACC.COM




SAVING THE COMPANY

ACC'S ANNUAL MEETING 2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT



DISCUSSION

ACC'S ANNUAL MEETING 2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT

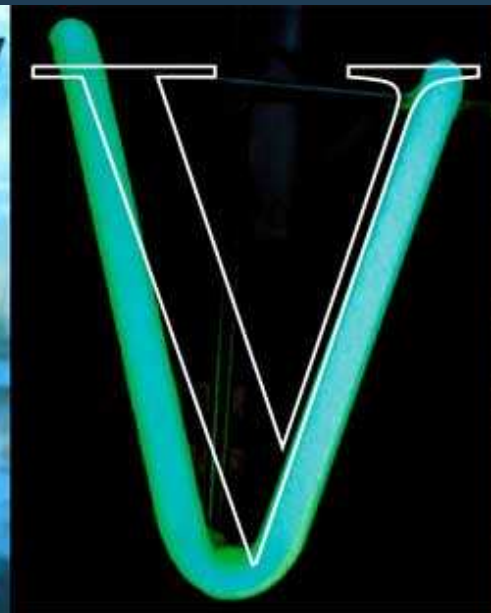
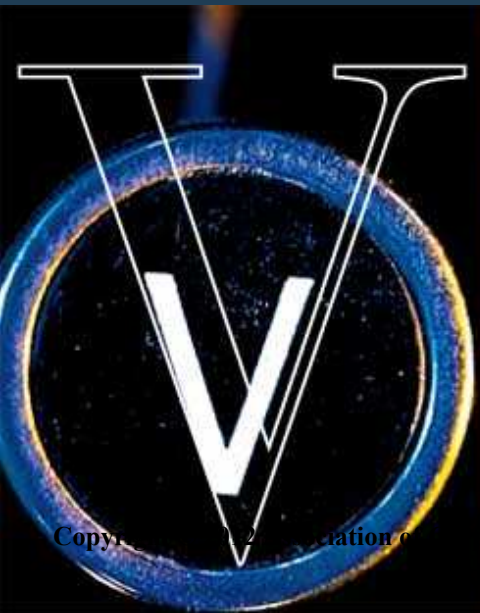


CONCLUDING THOUGHTS

VENABLE[®]_{LLP}

An Overview of Incident Response Plans for Security Breaches

July 2012



Purpose of an Incident Response Plan

- Purpose of the plan is to facilitate a prompt and coordinated response:
 - Prompt investigation of the incident;
 - Detection and prevention of ongoing activity;
 - Restoration of systems' security and integrity;
 - Prevention of the reoccurrence;
 - Notification and engagement of departments within the company;
 - Notification of external parties affected by the incident, if any, such as customers, associates, or credit card companies;
 - Notification of state or federal regulatory agencies, if required;
 - Notification of and cooperation with law enforcement officials, if deemed necessary; and
 - Prompt disclosure or financial reporting if required by federal or state securities laws.



What Should Your Incident Response Plan Contain?

- Designated incident lead
- Emergency contacts
- Internal reporting system to alert legal, senior management, communications, and others
- Information on relevant regulatory and law enforcement agencies that must be contacted
- Steps required to assess scope of breach and preparation of response



Designated Incident Lead

- One individual (and backup) designated to coordinate the response
- Should act as go-between for management and the response team
- Typically someone from Legal or Chief Privacy Officer
- Will coordinate efforts among all groups, notify appropriate people within the company and externally, document the response, identify key tasks and estimate costs



Emergency Contacts and Internal Reporting System

- Emergency Contact List should include
 - Representative(s) of executive management team
 - Legal, privacy & compliance
 - Operations (Security & IT)
 - Customer Service and/or HR
 - Communications/Public Relations
- Incident Response Plan should designate structure of internal reporting system



Law Enforcement Agencies

- If you believe the incident may have involved illegal activities, notify law enforcement of the breach
- Incident response plan should include contact info.
- Key law enforcement may include:
 - FBI
 - U.S. Secret Service
 - Local law enforcement



Assessing the Breach and Response

- Incident Plan should contain steps necessary to contain the breach and to conduct a preliminary internal assessment of the scope of the breach. Consider:
 - Isolating the affected system to prevent further release;
 - Activating auditing software;
 - Preserving pertinent system logs;
 - Making back-up copies of altered files to be kept secure;
 - Identifying systems that connect to the affected system;
 - Retaining an external third party to assist with the investigation;
 - Documenting conversations with law enforcement and steps taken to restore the integrity of the system.
- Incident response plan should also contain steps to undertake to provide prompt notice to affected individuals, if required



Assessing the Breach and Response, cont.

- Incident response plan should also contain guidelines to assess when the following may be required:
 - Notification to other third parties, such as insurance carriers, card holder associations, etc.;
 - Provision of an identity theft protection service, identity theft counseling and professional assistance;
 - Press strategy and press responses;
 - Public affairs and government affairs strategy.
- Incident response plan should also contain a plan post-notification to review events and make adjustments to technology and response plan to reflect lessons learned.



State Laws That Govern Breach Notification

- State breach notification laws (now in 46 states, DC, PR, Guam and USVI) generally require notification to individuals if their “personal information” was, or reasonably is, believed to have been acquired by an unauthorized person.
 - “Personal information” is commonly defined to include an individual’s name combined with a certain “data element” such as a Social Security number, driver’s license number, or account number in combination with any password that would permit access to a person’s account
 - State laws can have significant and conflicting variations
 - Some states include include medical information in their state data breach laws



When to Notify?

- Majority rule: notify “in the most expedient time possible and without unreasonable delay”
 - *Some states set minimum time limits for notice*
- May delay notification consistent with needs of law enforcement (except in IL)



Individual Notification Methods

- Via first-class mail
- Via e-mail, if individual has agreed to e-mail notice and has not withdrawn agreement
- Via phone, in some states
- Almost all states permit substitute notice if individual notice is particularly burdensome in terms of cost or number of individuals, often described as over 500k individuals and/or costing more than \$250k



Individual Notification Contents

- Some states specify particular language to be included in notice.
 - For example, MD requires toll-free numbers and addresses for credit reporting agencies, toll-free numbers, addresses, and websites for the FTC and state AG, and a statement that the individual can obtain information from these sources about steps to avoid identity theft.



Venable LLP

Important Steps in Minimizing Risk and Loss Related to Data Breaches

Bobby N. Turnage, Jr.

- I. Steps to Protect Against a Future Breach
 - a. Review current systems, physical facilities and processes for vulnerabilities
 - i. Consider hiring security consultant
 - b. Conduct regular security audits
 - c. Review contracts with relevant vendors and require specific reps and warranties around security
 - d. Performing appropriate due diligence around vendor systems and facilities to confirm security
 - e. Performing proper due diligence around acquisition target systems related to security
 - f. Ensure system updates and maintenance are performed timely
 - g. Training employees on security do's and don'ts
 - h. Maintaining an appropriate security policy (will address things like destruction of documents, safeguarding and destruction of computer [and copier] hard-drives, physical security, passwords, etc.)
 - i. Maintain top-down emphasis (from executive team) on security
- II. Steps to Minimize Potential Losses in the Event of a Breach
 - a. Maintain appropriate insurance coverages
 - i. Includes cyber-insurance
 1. Can cover cost related to investigation, notification, public relations, breach coach, law firm, defense costs, etc.
 - ii. Use a knowledgeable broker/consultant
 1. All policies are not the same (and neither are the brokers)
 - b. Prepare and maintain appropriate incident response plan

- c. Review privacy promises to ensure consistency with actual practices
 - d. Review contracts with relevant vendors and customers to ensure appropriate shifting of risks and insurance coverage related to data breach
 - e. Confirm insurance requirements of vendors
 - f. Public companies consider cyber-risk disclosure obligations
- III. Steps in the Event of a Breach to Minimize Losses and Increase Chances of a Better Result
- a. Isolate compromised systems, if applicable
 - b. Preserve relevant logs and other IT data
 - c. Activate incident response plan and notify relevant POC's
 - d. Retain data breach law firm
 - i. Law firm will be able to advise on notification obligations and messaging
 - 1. Notification may be required/recommended for relevant regulators (FTC, HHS, State AG's), law enforcement, credit bureaus, card holder associations and others
 - 2. Messaging to employees and customer base
 - ii. Law firm will be able to hire your forensic investigation firm to help protect privilege and work product (noted below)
 - iii. Law firm with experience and reputation with regulators will provide credibility in the event notification becomes necessary or regulatory investigation ensues
 - iv. Law firm with experience can help avoid missteps that will ultimately be scrutinized and second-guessed by others later
 - e. Consider public company disclosure obligations
 - f. Notify insurance carrier
 - i. Coordinate with carrier throughout
 - 1. Carrier may have experience to share
 - 2. Coordination reduces chances of misunderstanding leading to coverage issues

- g. Retain forensic firm for investigation and remedial measures – if breach of systems vs. stolen or lost data
 - i. Have law firm retain for privilege and work product protections
 - ii. Have forensic firm provide detailed scope of work and frequent invoices
 - 1. This ticket item can get expensive quickly
 - 2. Scope of needed work can change
- h. Add additional members to response team
 - i. Information Technology (internal)
 - ii. Public relations (internal and/or external)
 - iii. Customer service
 - iv. HR
- i. Advise internal groups to be careful with written communications
- j. Establish legal dept (or law firm) as the command center for coordination of all activities related to the breach

POLICY TEMPLATES

Aryeh Friedman
Chief Privacy Officer, Dun & Bradstreet

PRIVACY DATA BREACH RESPONSE POLICY**I. Initial Detection and Identification****1. Initial Detection:**

- a. How will the Privacy Office be notified about a Data Breach? You should have periodic dry runs to test the process
- b. Have Policy in place covering data breaches when data is in the hands of third parties.

2. Process for Scoping the Data Breach:

- a. Set out criteria for making the determination of whether an incident is a "Privacy Data Breach Incident" subject to the Policy
- b. Identify the relevant countries (in the US the relevant states) of residence of the affected data subjects to determine which laws may apply.
- c. Identify what data elements were compromised in any particular incident.
Elements you would be concerned about:
 - i. Social security number; driver's license number or a national or state identification number; it could also include date of birth.
 - ii. Financial account number, credit or debit card number, in conjunction with the applicable security access code or password;
 - iii. Personal Health Information (PHI) as defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or other medical information (including an individual's medical history, mental or physical condition, or medical treatment or diagnosis administered by a health care professional); health insurance information (including an individual's health insurance policy number, a unique identifier used by a health insurer, or any information regarding an individual's application and claims history).

II. First Response – Day 1:

1. **Set Timeline:** Determine the potentially applicable laws and determine the relevant time frames for notification.
2. **Recording the Incident** in whatever Case Management you use
3. **Internal Notifications:** The General Counsel, Corporate Communications
4. **Assemble an investigation team** using internal and if necessary external resources. Team Leader should be identified and roles assigned.

5. **Notification of Law Enforcement if appropriate.**
6. **Make sure you have a budget:** Process for identifying who is responsible for bearing the costs of the investigation and notifications and for making them aware of that.
7. **Invoke the Crisis Management Plan:** Link and coordinate your breach response with your company Crisis Management Plan (see below)
8. **Containment:** This includes: (i) what measures must be taken to contain the data breach; (ii) who are the parties responsible for taking those measures and (iii) the time table for implementation of those measures.

III. Investigation

1. **Privilege?**
2. **Investigation Team Meetings:** Regular schedule for meeting with your team with tight time frames. I would recommend daily meetings with update reports, and preparing “to do” lists for the next day. Accountability, accountability, accountability ...
3. **Interviews and Document Collection:** Investigator notes, documents should be maintained in a centralized location.
4. **Investigation Report:** It should include the following:
 - The chronology of the events that caused the Privacy Data Breach Incident.
 - Identification of all persons (including their state of residency and their contact information, if available) whose Reportable Personal Data Elements were exposed, and the specific data elements listed by person.
 - Determination as to whether the Breach is reportable and to whom
 - Reportable or not,
5. **Gap and Remediation Report:** Reportable or not, there should be a separate report on gaps identified and remediation measures recommended; learnings from the investigation.

IV. Notification and Reporting a Privacy Breach

1. **Reporting to Government Agencies:** Determine what government agencies or officials need to be notified and the contents of that notification.
2. **Affected Individual(s) Notifications**
 - a. Determine how individual notifications must be made in accordance with applicable law
 - b. Determine whether credit monitoring or other remedial measures are required or would be appropriate.

V. Post-Incident Review and Remediation

1. Implement the recommended Remediation measures
2. Post-Incident review/post-mortem of the Privacy Incident Response Procedure itself

CRISIS MANAGEMENT POLICY

Critical to have process defined before a crisis arises. Informed planning is critical.

1. **Scope and Outcomes Desired**
 - a. Identify what events trigger the plan, what events do not fall in scope. You should be able to anticipate potential crises. This should be updated regularly reflecting current issues/concerns.
 - b. What are the desired outcomes – what are the goals of your crisis management plan (if event specific, identify outcomes based on the crises anticipated by the plan)? What will you need to achieve those outcomes? Plan should be shaped by your desired outcomes.
 - c. For global companies, the same event may require a different process in different countries.
2. **Contact Information** for all potential participants in the plan (internal and external):
 - a. They should be kept in a centralized, accessible location and up-to-date
 - b. Contacts may be event specific; plan should identify the positions of the persons needed, and the current person sitting in that position. Process in place to automatically update when person in position replaced or position eliminated.
 - c. Dry runs to test process
3. **Roles and Responsibilities Defined:**
 - a. Internal and External Resources
 - b. Appropriate Teams for Specific Crises
 - c. Coordination and Sequencing/Handoffs
 - d. Accountability for and ownership of tasks and outcomes should be documented
4. **Day 1:** An initial realistic assessment based on available information
 - a. Fact versus rumor as of Day 1
 - b. Process to collect additional facts so that decision is made on the basis of facts on the ground.
5. **Daily Meetings** with reports, updated assessments, and “to-do” lists for the next day
6. **Clear Escalation Process:** To resolve the inevitable disputes
7. **Communications Plan** – Internal and External
 - a. Employees need to have a trusted source of information
 - b. Transparency externally as well.
8. **Event-Specific Gaps and Remediation:** Process should allow for event-specific gaps to be identified and remediation measures proposed and implemented.

9. **The Crisis Management Plan is a living document:** Have a post-mortem process to reevaluate how the crisis management plan worked, what gaps were identified, and what remediation is necessary to improve the process.

State Security Breach Notification Laws

States with no security breach law: Alabama, Kentucky, New Mexico, and South Dakota.

THIS DOCUMENT IS NOT INTENDED TO PROVIDE LEGAL ADVICE, OR TO BE A SUBSTANTIVE ANALYSIS OF STATE LAW PROVISIONS.

Not all provisions of the state statute have been reproduced here. Please refer to the state code for complete statutory language and other state-specific requirements.

Please see the National Conference of State Legislatures site for comprehensive information: <http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx>

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
Alabama	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION
Alaska	Alaska Stat. § 45.48.010 et seq.	If a covered person owns or licenses personal information in any form that includes personal information on a state resident, and a breach of the security of the information system that contains personal information occurs, the covered person shall, after discovering or being notified of the breach, disclose the breach to each state resident whose personal information was subject to the breach.	"personal information" means information in any form on an individual that is not encrypted or redacted, or is encrypted and the encryption key has been accessed or acquired, and that consists of a combination of (A) an individual's name; in this subparagraph, "individual's name" means a combination of an individual's (i) first name or first initial; and (ii) last name; and (B) one or more of the following information elements: (i) the individual's social security number; (ii) the individual's driver's license number or state identification card number; (iii) except as provided in (iv) of this subparagraph, the individual's account number, credit card number, or debit card number; (iv) if an account can only be accessed with a personal code, the number in (iii) of this subparagraph and the personal code; in this subparagraph, "personal code"	...in the most expeditious time possible and without unreasonable delay, except as provided in AS 45.48.020 and as necessary to determine the scope of the breach and restore the reasonable integrity of the information system	disclosure is not required if, after an appropriate investigation and after written notification to the attorney general of this state, the covered person determines that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach. The determination shall be documented in writing, and the documentation shall be maintained for five years. The notification required by this subsection may not be considered a public record open to inspection by the public.	An information collector shall make the disclosure required by AS 45.48.010 (1) by a written document sent to the most recent address the information collector has for the state resident; (2) by electronic means if the information collector's primary method of communication with the state resident is by electronic means or if making the disclosure by the electronic means is consistent with the provisions regarding electronic records and signatures required for notices legally required to be in writing under 15 U.S.C. 7001 et seq. (Electronic Signatures in Global and National Commerce Act); or (3) [by public notification].	if the information collector demonstrates that the cost of providing notice would exceed \$150,000, that the affected class of state residents to be notified exceeds 300,000, or that the information collector does not have sufficient contact information to provide notice, by: electronic mail if the information collector has an electronic mail address for the state resident; conspicuously posting the disclosure on the Internet website of the information collector if the information collector maintains an Internet website; and providing a notice to major statewide media.	(1) "breach of the security" means unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector; in this paragraph, "acquisition" includes acquisition by (A) photocopying, facsimile, or other paper-based method; (B) a device, including a computer, that can read, write, or store information that is represented in numerical form; or (C) a method not identified by (A) or (B) of this paragraph; (2) "covered person" means a (A) person doing business; (B) governmental agency; or (C) person with more than 10 employees; (3) "governmental agency" means a state or local governmental agency, except for an agency of the judicial

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/Substitute Notification	Some Definitions
			means a security code, an access code, a personal identification number, or a password; (v) passwords, personal identification numbers, or other access codes for financial accounts.					branch; (4) "information collector" means a covered person who owns or licenses personal information in any form if the personal information includes personal information on a state resident[.]
Arizona	Ariz. Rev. Stat. § 44-7501	When a person that conducts business in this state and that owns or licenses unencrypted computerized data that includes personal information becomes aware of an incident of unauthorized acquisition and access to unencrypted or unredacted computerized data that includes an individual's personal information, the person shall conduct a reasonable investigation to promptly determine if there has been a breach of the security system. If the investigation results in a determination that there has been a breach in the security system, the person shall notify the individuals affected. A person that maintains unencrypted computerized data that includes personal information that the person does not own shall notify and cooperate with the owner or the licensee of the information of any breach of the security of the system following discovery of the breach without unreasonable delay. Cooperation shall include sharing information relevant to the breach of the security of the system with the owner or licensee. The person that owns	6. "Personal information": (a) 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 the data element is not encrypted, redacted or secured by any other method rendering the element unreadable or unusable: (i) The individual's social security number. (ii) The individual's number on a driver license issued pursuant to section 28-3166 or number on a nonoperating identification license issued pursuant to section 28-3165. (iii) The individual's financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to the individual's financial account. (b) Does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.	The notice shall be made in the most expedient manner possible and without unreasonable delay subject to the needs of law enforcement as provided in subsection C of this section and any measures necessary to determine the nature and scope of the breach, to identify the individuals affected or to restore the reasonable integrity of the data system. The notification required by subsection A of this section may be delayed if a law enforcement agency advises the person that the notification will impede a criminal investigation. The person shall make the notification after the law enforcement agency determines that it will not compromise the investigation.	A person is not required to disclose a breach of the security of the system if the person or a law enforcement agency, after a reasonable investigation, determines that a breach of the security of the system has not occurred or is not reasonably likely to occur. This section does not apply to either of the following: 1. A person subject to title V of the Gramm-Leach-Bliley act of 1999 (P.L. 106-102; 113 Stat. 1338; 15 United States Code sections 6801 through 6809). 2. Covered entities as defined under regulations implementing the health insurance portability and accountability act, 45 Code of Federal Regulations section 160.103 (1996). The person that maintained the data under an agreement with the owner or licensee is not required to provide notice to the individual pursuant to this section unless the agreement stipulates otherwise.	The disclosure required by subsection A of this section shall be provided by one of the following methods: 1. Written notice. 2. Electronic notice if the person's primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in the electronic signatures in global and national commerce act (P.L. 106-229; 114 Stat. 464; 15 United States Code section 7001). 3. Telephonic notice. 4. Substitute notice if the person demonstrates that the cost of providing notice pursuant to paragraph 1, 2 or 3 of this subsection would exceed fifty thousand dollars or that the affected class of subject individuals to be notified exceeds one hundred thousand persons, or the person does not have sufficient contact information. A person who maintains the person's own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the requirements of this section shall be deemed to be in compliance with the notification requirements of this section if the person notifies subject individuals in accordance with the person's policies if a breach of the security system occurs. A person that complies with the notification requirements or security breach procedures pursuant to the rules, regulations, procedures, guidance or guidelines established by the person's primary or functional federal regulator is deemed to be in compliance with this section.	Substitute notice shall consist of all of the following: (a) Electronic mail notice if the person has electronic mail addresses for the individuals subject to the notice. (b) Conspicuous posting of the notice on the web site of the person if the person maintains one. (c) Notification to major statewide media.	"Breach", "breach of the security of the system", "breach of the security system" or "security breach" means an unauthorized acquisition of and access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of personal information maintained by a person as part of a database of personal information regarding multiple individuals and that causes or is reasonably likely to cause substantial economic loss to an individual. Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security system if the personal information is not used for a purpose unrelated to the person or subject to further wilful unauthorized disclosure. "Encrypted" means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		or licenses the computerized data shall provide notice to the individual pursuant to this section.						"Individual" means a person that is a resident of this state as determined by a principal mailing address in this state as reflected in the records of the person conducting business in this state at the time of the breach. "Person" means a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency or any other legal or commercial entity. Person does not include the department of public safety, a county sheriff's department, a municipal police department, a prosecution agency or a court.
Arkansas	Ark. Code § 4-110-101 et seq.	Any person or business that acquires, 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 of the security of the system to any resident of Arkansas whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	"Personal information" means an individual's first name or first initial and his or her last name in combination with any one (1) or more of the following data elements when either the name or the data element is not encrypted or redacted: (A) Social security number; (B) Driver's license number or Arkansas identification card number; (C) Account number, credit card number, 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; and (D) Medical information; (5) "Medical information"	The disclosure shall be made in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section, or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system. 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	Notification under this section is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers. Notwithstanding subsection (e) of this section, 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 section shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies affected persons in accordance with its policies in the event of a breach of the security of the system. The	For purposes of this section, notice may be provided by one (1) of the following methods: (1) Written notice; (2) Electronic mail notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001, as it existed on January 1, 2005; or (3) Substitute notice if the person or business demonstrates that: (i) The cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000); (ii) The affected class of persons to be notified exceeds five hundred thousand (500,000); or (iii) The person or business does not have sufficient contact information.	Substitute notice shall consist of all of the following: (i) Electronic mail notice when the person or business has an electronic mail address for the subject persons; (ii) Conspicuous posting of the notice on the website of the person or business if the person or business maintains a website; and (iii) Notification by statewide media.	"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 a person or business. "Breach of the security of the system" does not include the good faith acquisition of personal information by an employee or agent of the person or business for the legitimate purposes of the person or business if the personal information is not otherwise used or subject to further unauthorized disclosure; "Business" means a sole proprietorship, partnership,

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
			means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional; (6) "Owns or licenses" includes, but is not limited to, personal information that a business retains as part of the internal customer account of the business or for the purpose of using the information in transactions with the person to whom the information relates;	the law enforcement agency determines that it will not compromise the investigation.	provisions of this chapter do not apply to a person or business that is regulated by a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breaches of the security of personal information than that provided by this chapter. Compliance with the state or federal law shall be deemed compliance with this chapter with regard to the subjects covered by this chapter. This section does not relieve a person or business from a duty to comply with any other requirements of other state and federal law regarding the protection and privacy of personal information.			corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country or the parent or the subsidiary of a financial institution. "Business" includes: (i) An entity that destroys records; and (ii) A state agency; "Individual" means a natural person; "Records" means any material that contains sensitive personal information in electronic form. "Records" does not include any publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number; and "State agencies" or "state agency" means any agency, institution, authority, department, board, commission, bureau, council, or other agency of the State of Arkansas supported by cash funds or the appropriation of state or federal funds.
California	Cal. Civ. Code §§ 1798.29 [state	Any person or business that conducts business in California, and that owns or licenses	(h) For purposes of this section, "personal information" means an individual's first	The disclosure shall be made in the most expedient time possible and without	A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42	Any person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:	Substitute notice shall consist of all of the following:	For purposes of this section, "breach of the security of the system" means unauthorized

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
	agencies], 1798.80 et seq. [commercial entities]	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. 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.	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. (4) Medical information. (5) Health insurance information. (i) (1) 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. (2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. (3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any	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. 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.	U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section. Notwithstanding subdivision (j), 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.	(1) The security breach notification shall be written in plain language. (2) The security breach notification shall include, at a minimum, the following information: (A) The name and contact information of the reporting person or business subject to this section. (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach. (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice. (D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided. (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided. (F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number. (3) At the discretion of the person or business, the security breach notification may also include any of the following: (A) Information about what the person or business has done to protect individuals whose information has been breached. (B) Advice on steps that the person whose information has been breached may take to protect himself or herself. Any person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any	(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 Internet Web site page of the person or business, if the person or business maintains one. (C) Notification to major statewide media and the Office of Privacy Protection within the State and Consumer Services Agency.	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.

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
			unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records..			personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code. 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.		
Colorado	Colo. Rev. Stat. § 6-1-716	An individual or a commercial entity that conducts business in Colorado and that owns or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware of a breach of the security of the system, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the	(d) (I) "Personal information" means a Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable: (A) Social security number; (B) Driver's license number or identification card number; (C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial	The individual or the commercial entity shall give notice as soon as possible to the affected Colorado resident unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur. Notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable	Nothing in this paragraph (d) shall be construed to require the individual or commercial entity to provide to the consumer reporting agency the names or other personal information of breach notice recipients. [The requirement to notify consumer reporting agencies] shall not apply to a person who is subject to Title V of the federal "Gramm-Leach-Bliley Act", 15 U.S.C. sec. 6801 et seq. [A]n individual or a commercial entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information and whose procedures are otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notice	(c) "Notice" means: (I) Written notice to the postal address listed in the records of the individual or commercial entity; (II) Telephonic notice; (III) Electronic notice, if a primary means of communication by the individual or commercial entity with a Colorado resident is by electronic means or the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. sec. 7001 et seq.; or (IV) Substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed two hundred fifty thousand dollars, the affected class of persons to be notified exceeds two hundred fifty thousand Colorado residents, or the individual or the commercial entity does not have sufficient contact information to provide notice.	Substitute notice consists of all of the following: (A) E-mail notice if the individual or the commercial entity has e-mail addresses for the members of the affected class of Colorado residents; (B) Conspicuous posting of the notice on the web site page of the individual or the commercial entity if the individual or the commercial entity maintains one; and (C) Notification to major statewide media.	(a) "Breach of the security of the system" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an individual or commercial entity for the purposes of the individual or commercial entity is not a breach of the security of the system if the personal information is not used for or is not subject to further unauthorized disclosure.

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>security of the system immediately following discovery of a breach, if misuse of personal information about a Colorado resident occurred or is likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach; except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets.</p>	<p>account. (II) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.</p>	<p>integrity of the computerized data system. Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation and the law enforcement agency has notified the individual or commercial entity that conducts business in Colorado not to send notice required by this section. Notice required by this section shall be made in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation and has notified the individual or commercial entity that conducts business in Colorado that it is appropriate to send the notice required by this section. (d) If an individual or commercial entity is required to notify more than one thousand Colorado residents of a breach of the security of the system pursuant to this section, the individual or commercial entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and</p>	<p>requirements of this section if the individual or the commercial entity notifies affected Colorado customers in accordance with its policies in the event of a breach of security of the system. (b) An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section.</p>			

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
				maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. sec. 1681a (p), of the anticipated date of the notification to the residents and the approximate number of residents who are to be notified.				
Connecticut	Conn. Gen Stat. 36a-701b	<p>Any person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information, shall provide notice of any breach of security following the discovery of the breach to any resident of this state whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person through such breach of security.</p> <p>Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following its discovery, if the personal information of a resident of this state was, or is reasonably believed to have been accessed by an unauthorized person.</p>	"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: (1) Social Security number; (2) driver's license number or state identification card number; or (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. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.	Such [disclosure] notice shall be made without unreasonable delay, subject to the provisions of subsection (d) of this section and the completion of an investigation by such person to determine the nature and scope of the incident, to identify the individuals affected, or to restore the reasonable integrity of the data system. Such notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed. Any notification required by this section shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a	Any person that maintains such person's own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of this section, shall be deemed to be in compliance with the security breach notification requirements of this section, provided such person notifies, as applicable, residents of this state, owners and licensees in accordance with such person's policies in the event of a breach of security and in the case of notice to a resident, such person also notifies the Attorney General not later than the time when notice is provided to the resident. Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator, as defined in 15 USC 6809(2), shall be deemed to be in compliance with the security breach notification requirements of this section, provided (1) such person notifies, as applicable, such residents of this state, owners, and licensees	Any notice to a resident, owner or licensee required by the provisions of this section may be provided by one of the following methods: (1) Written notice; (2) telephone notice; (3) electronic notice, provided such notice is consistent with the provisions regarding electronic records and signatures set forth in 15 USC 7001; (4) substitute notice, provided such person demonstrates that the cost of providing notice in accordance with subdivision (1), (2) or (3) of this subsection would exceed two hundred fifty thousand dollars, that the affected class of subject persons to be notified exceeds five hundred thousand persons or that the person does not have sufficient contact information.	Substitute notice shall consist of the following: (A) Electronic mail notice when the person has an electronic mail address for the affected persons; (B) conspicuous posting of the notice on the web site of the person if the person maintains one; and (C) notification to major state-wide media, including newspapers, radio and television.	"breach of security" means unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable;

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
				<p>criminal investigation and such law enforcement agency has made a request that the notification be delayed. Any such delayed notification shall be made after such law enforcement agency determines that notification will not compromise the criminal investigation and so notifies the person of such determination.</p> <p>[Effective Oct 1, 2012] If notice of a breach of security is required by subdivision (1) of this subsection, the person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information, shall not later than the time when notice is provided to the resident also provide notice of the breach of security to the Attorney General.</p>	<p>required to be notified under and in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or functional regulator in the event of a breach of security, and (2) if notice is given to a resident of this state in accordance with subdivision (1) of this subsection regarding a breach of security, such person also notifies the Attorney General not later than the time when notice is provided to the resident.</p>			
Delaware	Del. Code tit. 6, § 12B-101 et seq.	An individual or a commercial entity that conducts business in Delaware and that owns or licenses computerized data that includes personal information about a resident of Delaware shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the	"Personal information" means a Delaware resident's first name or first initial and last name in combination with any 1 or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted: a. Social Security number; b. Driver's license number or	If the investigation determines that the misuse of information about a Delaware resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected Delaware resident. Notice must be made in the most	Under this chapter, an individual or a commercial entity that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notice requirements of this	"Notice" means: a. Written notice; b. Telephonic notice; c. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 of Title 15 of the United States Code; or d. Substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed \$75,000, or that the affected class of	Substitute notice consists of all of the following: 1. E-mail notice if the individual or the commercial entity has e-mail addresses for the members of the affected class of Delaware residents; and	"Breach of the security of the system" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Good faith acquisition of personal information by an

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>likelihood that personal information has been or will be misused.</p> <p>An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach, if misuse of personal information about a Delaware resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach.</p>	<p>Delaware Identification Card number; or</p> <p>c. Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.</p> <p>The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records;</p>	<p>expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.</p> <p>Notice required by this chapter may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by this chapter must be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.</p>	<p>chapter if the individual or the commercial entity notifies affected Delaware residents in accordance with its policies in the event of a breach of security of the system.</p> <p>(b) Under this chapter, an individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this chapter if the individual or the commercial entity notifies affected Delaware residents in accordance with the maintained procedures when a breach occurs.</p>	<p>Delaware residents to be notified exceeds 100,000 residents, or that the individual or the commercial entity does not have sufficient contact information to provide notice.</p>	<p>2. Conspicuous posting of the notice on the web site page of the individual or the commercial entity if the individual or the commercial entity maintains one; and</p> <p>3. Notice to major statewide media.</p>	<p>employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure;</p> <p>(2) "Commercial entity" includes corporations, business trusts, estates, trusts, partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit;</p>
Florida	Fla. Stat. § 817.5681	<p>Any person who conducts business in this state and maintains computerized data in a system that includes personal information shall provide notice of any breach of the security of the system, following a determination of the breach, to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>Any person who maintains computerized data that includes personal information on behalf of</p>	<p>"personal information" means an individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements when the data elements are not encrypted:</p> <p>(a) Social security number.</p> <p>(b) Driver's license number or Florida Identification Card number.</p> <p>(c) Account number, credit card number, or debit card number, in combination with any required security code,</p>	<p>The notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3) and paragraph (10)(a), or subject to any measures necessary to determine the presence, nature, and scope of the breach and restore the reasonable integrity of the system.</p> <p>Notification must be made no later than 45 days following the determination</p>	<p>a person who maintains:</p> <p>(a) The person's own notification procedures as part of an information security or privacy policy for the treatment of personal information, which procedures are otherwise consistent with the timing requirements of this part; or</p> <p>(b) A notification procedure pursuant to the rules, regulations, procedures, or guidelines established by the person's primary or functional federal regulator, shall be deemed to be in compliance with the notification</p>	<p>notice may be provided by one of the following methods:</p> <p>(a) Written notice;</p> <p>(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. s. 7001 or if the person or business providing the notice has a valid e-mail address for the subject person and the subject person has agreed to accept communications electronically; or</p> <p>(c) Substitute notice, if the person demonstrates that the cost of providing notice would exceed \$250,000, the affected class of subject persons to be notified exceeds 500,000, or the person does not have sufficient contact information.</p>	<p>Substitute notice shall consist of all of the following:</p> <p>1. Electronic mail or e-mail notice when the person has an electronic mail or e-mail address for the subject persons.</p> <p>2. Conspicuous posting of the notice on the web page of the person, if the person maintains a web page.</p> <p>3. Notification to major</p>	<p>"breach" and "breach of the security of the system" mean unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person.</p> <p>Good faith acquisition of personal information by an employee or agent of the person is not a breach or breach of the security of the system, provided the information is not used for a</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>another business entity shall disclose to the business entity for which the information is maintained any breach of the security of the system as soon as practicable, but no later than 10 days following the determination, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>access code, or password that would permit access to an individual's financial account. For purposes of this section, the term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.</p>	<p>of the breach unless otherwise provided in this section. (b) Any person required to make notification under paragraph (a) who fails to do so within [the time period prescribed] following the determination of a breach or receipt of notice from law enforcement as provided in subsection (3) is liable for an administrative fine not to exceed \$500,000.... ***</p> <p>The notification required by this section may be delayed upon a request by law enforcement if a law enforcement agency determines that the notification will impede a criminal investigation. The notification time period required by this section shall commence after the person receives notice from the law enforcement agency that the notification will not compromise the investigation.</p> <p>If a person discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at a single time, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers</p>	<p>requirements of this section if the person notifies subject persons in accordance with the person's policies or the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security of the system.</p> <p>Notification is not required if, after an appropriate investigation or after consultation with relevant federal, state, and local agencies responsible for law enforcement, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed. Such a determination must be documented in writing and the documentation must be maintained for 5 years.</p> <p>Any person required to document a failure to notify affected persons who fails to document the failure as required in this subsection or who, if documentation was created, fails to maintain the documentation for the full 5 years as required in this subsection is liable for an administrative fine in the amount of up to \$50,000 for such failure. ***</p>		<p>statewide media.</p>	<p>purpose unrelated to the business or subject to further unauthorized use. "unauthorized person" means any person who does not have permission from, or a password issued by, the person who stores the computerized data to acquire such data, but does not include any individual to whom the personal information pertains. (8) For purposes of this section, the term "person" means a person as defined in s. 1.01(3). For purposes of this section, the State of Florida, as well as any of its agencies or political subdivisions, and any of the agencies of its political subdivisions, constitutes a person.</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
				on a nationwide basis, as defined in 15 U.S.C. s. 1681a(p), of the timing, distribution, and content of the notices.				
Georgia	Ga. Code §§ 10-1-910 - 10-1-912	Any information broker or data collector that maintains computerized data that includes personal information of individuals shall give notice of 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 this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Any person or business that maintains computerized data on behalf of an information broker or data collector that includes personal information of individuals that the person or business does not own shall notify the information broker or data collector of any breach of the security of the system within 24 hours following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	“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 or redacted: (A) Social security number; (B) Driver’s license number or state identification card number; (C) Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords; (D) Account passwords or personal identification numbers or other access codes; or (E) Any of the items contained in subparagraphs (A) through (D) of this paragraph when not in connection with the individual’s first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised. The term “personal information” does not include publicly available information	(a) The notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this Code section, or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The notification required by this Code section may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation. The notification required by this Code section shall be made after the law enforcement agency determines that it will not compromise the investigation.	Notwithstanding any provision of this paragraph to the contrary, an information broker or data collector 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 article shall be deemed to be in compliance with the notification requirements of this article if it notifies the individuals who are the subjects of the notice in accordance with its policies in the event of a breach of the security of the system.	“Notice” means: (A) Written notice; (B) Telephone notice; (C) 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; or (D) Substitute notice, if the information broker or data collector demonstrates that the cost of providing notice would exceed \$50,000.00, that the affected class of individuals to be notified exceeds 100,000, or that the information broker or data collector does not have sufficient contact information to provide written or electronic notice to such individuals. In the event that an information broker or data collector discovers circumstances requiring notification pursuant to this Code section of more than 10,000 residents of this state at one time, the information broker or data collector shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nation-wide basis, as defined by 15 U.S.C. Section 1681a, of the timing, distribution, and content of the notices.	(i) E-mail notice, if the information broker or data collector has an e-mail address for the individuals to be notified; (ii) Conspicuous posting of the notice on the information broker’s or data collector’s website page, if the information broker or data collector maintains one; and (iii) Notification to major state-wide media.	“Breach of the security of the system” means unauthorized acquisition of an individual’s electronic data that compromises the security, confidentiality, or integrity of personal information of such individual maintained by an information broker or data collector. Good faith acquisition or use of personal information by an employee or agent of an information broker or data collector for the purposes of such information broker or data collector is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
Hawaii	Haw. Rev. Stat. § 487N-1, -2	Any business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal information for specific government purposes shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. Any business located in Hawaii or any business that conducts business in Hawaii that maintains or possesses records or data containing personal information of residents of Hawaii that the business does not own or license, or any government agency that maintains or possesses records or data containing personal information of residents of Hawaii shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subsection (c).	that is lawfully made available to the general public from federal, state, or local government records. "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 Hawaii identification card number; or (3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.	The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data system. In the event a business provides notice to more than one thousand persons at one time pursuant to this section, the business shall notify in writing, without unreasonable delay, the State of Hawaii's office of consumer protection and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. section 1681a(p), of the timing, distribution, and content of the notice. The notice required by this section shall be delayed if a law enforcement agency informs the business or	The following businesses shall be deemed to be in compliance with this section: (1) A financial institution that is subject to the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice published in the Federal Register on March 29, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, or subject to 12 C.F.R. Part 748, and any revisions, additions, or substitutions relating to the interagency guidance; and (2) Any health plan or healthcare provider that is subject to and in compliance with the standards for privacy or individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996.	The notice shall be clear and conspicuous. The notice shall include a description of the following: (1) The incident in general terms; (2) The type of personal information that was subject to the unauthorized access and acquisition; (3) The general acts of the business or government agency to protect the personal information from further unauthorized access; (4) A telephone number that the person may call for further information and assistance, if one exists; and (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. For purposes of this section, notice to affected persons may be provided by one of the following methods: (1) Written notice to the last available address the business or government agency has on record; (2) Electronic mail notice, for those persons for whom a business or government agency has a valid electronic mail address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. section 7001; (3) Telephonic notice, provided that contact is made directly with the affected persons; and (4) Substitute notice, if the business or government agency demonstrates that the cost of providing notice would exceed \$100,000 or that the affected class of subject persons to be notified exceeds two hundred thousand, or if the business or government agency does not have sufficient contact information or consent to satisfy paragraph (1), (2), or (3), for only those affected persons without sufficient contact information or consent, or	Substitute notice shall consist of all the following: (A) Electronic mail notice when the business or government agency has an electronic mail address for the subject persons; (B) Conspicuous posting of the notice on the website page of the business or government agency, if one is maintained; and (C) Notification to major statewide media.	"Business" means a sole proprietorship, partnership, corporation, association, or other group, however organized, and whether or not organized to operate at a profit. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of the State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. The term also includes an entity whose business is records destruction. "Encryption" or "encrypted" means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key. "Government agency" means any department, division, board, commission, public corporation, or other agency or instrumentality of the State or of any county. "Records" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
				government agency that notification may impede a criminal investigation or jeopardize national security and requests a delay; provided that such request is made in writing, or the business or government agency documents the request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicates to the business or government agency its determination that notice will no longer impede the investigation or jeopardize national security.		if the business or government agency is unable to identify particular affected persons, for only those unidentifiable affected persons.		characteristics. "Security breach" means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach; provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.
Idaho	Idaho Stat. §§ 28-51-104 to 28-51-107	Disclosure of breach of security of computerized personal information by an agency, individual or a commercial entity. (1) A city, county or state agency, individual or a commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho shall, when it becomes aware of a breach of	(5) "Personal information" means an Idaho resident's first name or first initial and last name in combination with any one (1) or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted: (a) Social security number; (b) Driver's license number or Idaho identification card	Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the	Procedures deemed in compliance with security breach requirements. (1) An agency, individual or a commercial entity that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of section 28-51-105, Idaho Code, is deemed to be in	(4) "Notice" means: (a) Written notice to the most recent address the agency, individual or commercial entity has in its records; (b) Telephonic notice; (c) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. section 7001; or (d) Substitute notice, if the agency, individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will	Substitute notice consists of all of the following: (i) E-mail notice if the agency, individual or the commercial entity has e-mail addresses for the affected Idaho residents; and (ii) Conspicuous posting of the notice on the website page of	"Breach of the security of the system" means the illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one (1) or more persons maintained by an agency, individual or a commercial entity. Good faith acquisition of personal

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur, the agency, individual or the commercial entity shall give notice as soon as possible to the affected Idaho resident.</p> <p>An agency, individual or a commercial entity that maintains computerized data that includes personal information that the agency, individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach, if misuse of personal information about an Idaho resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach.</p>	<p>number; or (c) Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account. The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.</p>	<p>reasonable integrity of the computerized data system. When an agency becomes aware of a breach of the security of the system, it shall, within twenty-four (24) hours of such discovery, notify the office of the Idaho attorney general. Nothing contained herein relieves a state agency's responsibility to report a security breach to the office of the chief information officer within the department of administration, pursuant to the information technology resource management council policies. Notice required by this section may be delayed if a law enforcement agency advises the agency, individual or commercial entity that the notice will impede a criminal investigation. Notice required by this section must be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency advises the agency, individual or commercial entity that notification will no longer impede the investigation.</p>	<p>compliance with the notice requirements of section 28-51-105, Idaho Code, if the agency, individual or the commercial entity notifies affected Idaho residents in accordance with its policies in the event of a breach of security of the system. An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with section 28-51-105, Idaho Code, if the individual or the commercial entity complies with the maintained procedures when a breach of the security of the system occurs.</p>	<p>exceed twenty-five thousand dollars (\$25,000), or that the number of Idaho residents to be notified exceeds fifty thousand (50,000), or that the agency, individual or the commercial entity does not have sufficient contact information to provide notice.</p>	<p>the agency, individual or the commercial entity if the agency, individual or the commercial entity maintains one; and (iii) Notice to major statewide media.</p>	<p>information by an employee or agent of an agency, individual or a commercial entity for the purposes of the agency, individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure. (6) "Primary regulator" of a commercial entity or individual licensed or chartered by the United States is that commercial entity's or individual's primary federal regulator, the primary regulator of a commercial entity or individual licensed by the department of finance is the department of finance, the primary regulator of a commercial entity or individual licensed by the department of insurance is the department of insurance and, for all agencies and all other commercial entities or individuals, the primary regulator is the attorney general.</p>
Illinois	815 ILCS 530/1 et seq.	Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a	"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	The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any	Notwithstanding any other subsection in this Section, a data collector that maintains its own notification procedures as part of an information security policy for	The disclosure notification to an Illinois resident shall include, but need not be limited to, (i) the toll-free numbers and addresses for consumer reporting agencies, (ii) the toll-free number, address, and website address for the Federal	Substitute notice shall consist of all of the following: (i) email notice if the data collector has an email	"Data Collector" may include, but is not limited to, government agencies, public and private universities, privately and publicly held

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/Substitute Notification	Some Definitions
		breach of the security of the system data following discovery or notification of the breach. Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license 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. In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach.	elements, when either the name or the data elements are not encrypted or redacted: (1) Social Security number. (2) Driver's license number or State identification card number. (3) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records.	measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation.	the treatment of personal information and is otherwise consistent with the timing requirements of this Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data.	Trade Commission, and (iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes. The notification shall not, however, include information concerning the number of Illinois residents affected by the breach. For purposes of this Section, notice to consumers 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 for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or (3) substitute notice, if the data collector demonstrates that the cost of providing notice would exceed \$250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information.	address for the subject persons; (ii) conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; and (iii) notification to major statewide media.	corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information. "Breach of the security of the system data" or "breach" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. "Breach of the security of the system data" does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.
Indiana	Ind. Code §§ 24-4.9 et seq. [commercial entities] [Note that 4-1-11 et seq. applies to governmental agencies]	a) Except as provided in section 4(c), 4(d), and 4(e) of this chapter, after discovering or being notified of a breach of the security of data, the data base owner shall disclose the breach to an Indiana resident whose: (1) unencrypted personal information was or may have been acquired by an unauthorized person; or (2) encrypted personal information was or may have been acquired by an	"Personal information" "Personal information" means: (1) a Social Security number that is not encrypted or redacted; or (2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted: (A) A driver's license number. (B) A state identification card number.	(a) A person required to make a disclosure or notification under this chapter shall make the disclosure or notification without unreasonable delay. (b) A person required to make a disclosure or notification under this chapter shall make the disclosure or notification as soon as possible after: (1) delay is no longer necessary to restore the	(c) A data base owner that maintains its own disclosure procedures as part of an information privacy policy or a security policy is not required to make a separate disclosure under this chapter if the data base owner's information privacy policy or security policy is at least as stringent as the disclosure requirements described in: (1) sections 1 through 4(b) of this chapter; (2) subsection (d); or	(a) Except as provided in subsection (b), a data base owner required to make a disclosure under this chapter shall make the disclosure using one (1) of the following methods: (1) Mail. (2) Telephone. (3) Facsimile (fax). (4) Electronic mail, if the data base owner has the electronic mail address of the affected Indiana resident. (b) If a data base owner required to make a disclosure under this chapter is required to make the disclosure to more than five hundred thousand (500,000) Indiana residents, or if the data base	[Substitute notice consists of] both of the following methods: (1) Conspicuous posting of the notice on the web site of the data base owner, if the data base owner maintains a web site. (2) Notice to major news reporting media in the geographic area where Indiana residents affected by	"Breach of the security of data" Sec. 2. (a) "Breach of the security of data" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>unauthorized person with access to the encryption key; if the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in IC 35-43-5-3.5), identity theft, or fraud affecting the Indiana resident. A data base owner required to make a disclosure under subsection (a) to more than one thousand (1,000) consumers shall also disclose to each consumer reporting agency (as defined in 15 U.S.C. 1681a(p)) information necessary to assist the consumer reporting agency in preventing fraud, including personal information of an Indiana resident affected by the breach of the security of a system.</p> <p>(c) If a data base owner makes a disclosure described in subsection (a), the data base owner shall also disclose the breach to the attorney general.</p>	<p>(C) A credit card number. (D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account. The term does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public.</p>	<p>integrity of the computer system or to discover the scope of the breach; or (2) the attorney general or a law enforcement agency notifies the person that delay will no longer impede a criminal or civil investigation or jeopardize national security. For purposes of this section, a delay is reasonable if the delay is:</p> <p>(1) necessary to restore the integrity of the computer system; (2) necessary to discover the scope of the breach; or (3) in response to a request from the attorney general or a law enforcement agency to delay disclosure because disclosure will:</p> <p>(A) impede a criminal or civil investigation; or (B) jeopardize national security.</p>	<p>(3) subsection (e). (d) A data base owner that maintains its own disclosure procedures as part of an information privacy, security policy, or compliance plan under:</p> <p>(1) the federal USA PATRIOT Act (P.L. 107-56); (2) Executive Order 13224; (3) the federal Driver's Privacy Protection Act (18 U.S.C. 2781 et seq.); (4) the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); (5) the federal Financial Modernization Act of 1999 (15 U.S.C. 6801 et seq.); or (6) the federal Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191);</p> <p>is not required to make a disclosure under this chapter if the data base owner's information privacy, security policy, or compliance plan requires that Indiana residents be notified of a breach of the security of data without unreasonable delay and the data base owner complies with the data base owner's information privacy, security policy, or compliance plan.</p> <p>(e) A financial institution that complies with the disclosure requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice or the Guidance on Response Programs for Unauthorized Access</p>	<p>owner required to make a disclosure under this chapter determines that the cost of the disclosure will be more than two hundred fifty thousand dollars (\$250,000), the data base owner required to make a disclosure under this chapter may elect to make the disclosure by using [substitute notice].</p> <p>(f) A person required to make a disclosure under this chapter may elect to make all or part of the disclosure in accordance with subsection (a) even if the person could make the disclosure in accordance with subsection (b).</p>	<p>the breach of the security of a system reside.</p>	<p>similar medium, even if the transferred data are no longer in a computerized format. (b) The term does not include the following:</p> <p>(1) Good faith acquisition of personal information by an employee or agent of the person for lawful purposes of the person, if the personal information is not used or subject to further unauthorized disclosure. (2) Unauthorized acquisition of a portable electronic device on which personal information is stored, if all personal information on the device is protected by encryption and the encryption key:</p> <p>(A) has not been compromised or disclosed; and (B) is not in the possession of or known to the person who, without authorization, acquired or has access to the portable electronic device. Data are encrypted for purposes of this article if the data:</p> <p>(1) have been transformed through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key; or (2) are secured by another method that renders the data unreadable or unusable. (a) Data are redacted for</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
					to Member Information and Member Notice, as applicable, is not required to make a disclosure under this chapter.			purposes of this article if the data have been altered or truncated so that not more than the last four (4) digits of: (1) a driver's license number; (2) a state identification number; or (3) an account number; is accessible as part of personal information. (b) For purposes of this article, personal information is "redacted" if the personal information has been altered or truncated so that not more than five (5) digits of a Social Security number are accessible as part of personal information.
Iowa	Iowa Code § 715C.1-715C.2	Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities and that was subject to a breach of security shall give notice of the breach of security following discovery of such breach of security, or receipt of notification under subsection 2, to any consumer whose personal information was included in the information that was breached. Any person who maintains or otherwise possesses personal information on behalf of another person shall notify the owner or licensor of the information of any breach of security immediately following discovery of such	11. "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 that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable: a. Social security number. b. Driver's license number or other unique identification number created or collected by a government body. c. Financial account number, credit card number, or debit card number in combination with any required security code, access code, or	The consumer notification shall be made in the most expeditious manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection 3, and consistent with any measures necessary to sufficiently determine contact information for the affected consumers, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data. The consumer notification requirements of this section may be delayed if a law	Notwithstanding subsection 1, notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determined that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years. This section does not apply to any of the following: a. A person who complies with notification requirements or breach of security procedures that provide greater protection to personal information and at least as	For purposes of this section, notification to the consumer may be provided by one of the following methods: a. Written notice to the last available address the person has in the person's records. b. Electronic notice if the person's customary method of communication with the consumer is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in chapter 554D and the federal Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001. c. Substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, that the affected class of consumers to be notified exceeds three hundred fifty thousand persons, or if the person does not have sufficient contact information to provide notice. Notice pursuant to this section shall include, at a minimum, all of the following: a. A description of the breach of security.	Substitute notice shall consist of the following: (1) Electronic mail notice when the person has an electronic mail address for the affected consumers. (2) Conspicuous posting of the notice or a link to the notice on the internet website of the person if the person maintains an internet website. (3) Notification to major statewide media.	1. "Breach of security" means unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information. 12. "Redacted" means altered

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		breach of security if a consumer's personal information was included in the information that was breached.	password that would permit access to an individual's financial account. d. Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account. e. Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data. "Personal information" does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public.	enforcement agency determines that the notification will impede a criminal investigation and the agency has made a written request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that the notification will not compromise the investigation and notifies the person required to give notice in writing.	thorough disclosure requirements than that provided by this section pursuant to the rules, regulations, procedures, guidance, or guidelines established by the person's primary or functional federal regulator. b. A person who complies with a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breach of security or personal information than that provided by this section. c. A person who is subject to and complies with regulations promulgated pursuant to Title V of the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6801 – 6809.	b. The approximate date of the breach of security. c. The type of personal information obtained as a result of the breach of security. d. Contact information for consumer reporting agencies. e. Advice to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general.		or truncated so that no more than five digits of a social security number or the last four digits of other numbers designated in section 715A.8, subsection 1, paragraph "a", are accessible as part of the data.
Kansas	Kan. Stat. 50-7a01, 50-7a02	(a) A person that conducts business in this state, or a government, governmental subdivision or agency that owns or licenses computerized data that includes personal information shall, when it becomes aware of any breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. An individual or a commercial entity that maintains computerized data that includes	(g) "Personal information" means a consumer's first name or first initial and last name linked to any one or more of the following data elements that relate to the consumer, when the data elements are neither encrypted nor redacted: (1) Social security number; (2) driver's license number or state identification card number; or (3) financial account number, or credit or debit card number, alone or in combination with any required security code, access code or password that	If the investigation determines that the misuse of information has occurred or is reasonably likely to occur, the person or government, governmental subdivision or agency shall give notice as soon as possible to the affected Kansas resident. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the	Notwithstanding any other provision in this section, an individual or a commercial entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section if the individual or the commercial entity notifies affected consumers in accordance with its policies in the event of a breach of security of the system.	(c) "Notice" means: (1) Written notice; (2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001; or (3) substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed \$100,000, or that the affected class of consumers to be notified exceeds 5,000, or that the individual or the commercial entity does not have sufficient contact information to provide notice. In the event that a person discovers circumstances requiring notification pursuant to this section of more than 1,000 consumers at one time, the person shall also notify, without unreasonable	(e) "Substitute notice" means: (1) E-mail notice if the individual or the commercial entity has e-mail addresses for the affected class of consumers; (2) conspicuous posting of the notice on the web site page of the individual or the commercial entity if the individual or the commercial entity maintains a web site; and (3) notification to	(a) "Consumer" means an individual who is a resident of this state. (b) "Encrypted" means transformation of data through the use of algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable. (h) "Security breach" means the unauthorized access and acquisition of unencrypted or unredacted computerized data

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/Substitute Notification	Some Definitions
		personal information that the individual or the commercial entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the data following discovery of a breach, if the personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.	would permit access to a consumer's financial account. The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.	scope of the breach and to restore the reasonable integrity of the computerized data system. Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by this section shall be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.	(e) An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section. This section does not relieve an individual or a commercial entity from a duty to comply with other requirements of state and federal law regarding the protection and privacy of personal information.	delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a(p), of the timing, distribution and content of the notices.	major statewide media.	that compromises the security, confidentiality or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity reasonably believes has caused or will cause, identity theft to any consumer. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used for or is not subject to further unauthorized disclosure.
Kentucky	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION
Louisiana	La. Rev. Stat. § 51:3071 et seq.	Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, shall, following discovery of a breach in the security of the system containing such data, notify any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. B. Any agency or person that maintains computerized data that includes personal information	(4)(a) "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 the name or the data element is not encrypted or redacted: (i) Social security number. (ii) Driver's license number. (iii) 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. (b) "Personal information" shall not include publicly	The notification required pursuant to Subsections A and B of this Section shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in Subsection D of this Section, or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system. If a law enforcement agency determines that the	Notification under this title is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers. A financial institution that is subject to and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the office of the comptroller of the currency and the office of thrift	Notification may be provided by one of the following methods: (1) Written notification. (2) Electronic notification, if the notification provided is consistent with the provisions regarding electronic records and signatures set forth in 15 USC 7001. (3) Substitute notification, if an agency or person demonstrates that the cost of providing notification would exceed two hundred fifty thousand dollars, or that the affected class of persons to be notified exceeds five hundred thousand, or the agency or person does not have sufficient contact information. Notwithstanding Subsection E of this Section, an agency or person that maintains a notification procedure as part of its information security policy for the treatment of personal information which is otherwise consistent with the timing requirements	Substitute notification shall consist of all of the following: (a) E-mail notification when the agency or person has an e-mail address for the subject persons. (b) Conspicuous posting of the notification on the Internet site of the agency or person, if an Internet site is maintained. (c) Notification to major statewide media.	(2) "Breach of the security of the system" means the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information maintained by an agency or person. Good faith acquisition of personal information by an employee or agent of an agency or person for the purposes of the agency or person is not a breach of the security of the system, provided that the personal

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		that the agency or person does not own shall notify the owner or licensee of the information if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person through a breach of security of the system containing such data, following discovery by the agency or person of a breach of security of the system.	available information that is lawfully made available to the general public from federal, state, or local government records.	notification required under this Section would impede a criminal investigation, such notification may be delayed until such law enforcement agency determines that the notification will no longer compromise such investigation.	supervision, and any revisions, additions, or substitutions relating to said interagency guidance, shall be deemed to be in compliance with this Chapter.	of this Section shall be deemed to be in compliance with the notification requirements of this Section if the agency or person notifies subject persons in accordance with the policy and procedure in the event of a breach of security of the system. LA Adm Code: When notice to Louisiana citizens is required pursuant to R.S. 51:3074, the person or agency shall provide written notice detailing the breach of the security of the system to the Consumer Protection Section of the Attorney General's Office. Notice shall include the names of all Louisiana citizens affected by the breach.		information is not used for, or is subject to, unauthorized disclosure.
Maine	Me. Rev. Stat. tit. 10 §§ 1347 et seq.	If an information broker that maintains computerized data that includes personal information becomes aware of a breach of the security of the system, the information broker shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State whose personal information has been, or is reasonably believed to have been, acquired by an unauthorized person. If any other person who maintains computerized data that includes personal information becomes aware of a breach of the security of the system, the person shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be	"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 or redacted: A. Social security number; B. Driver's license number or state identification card number; C. Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords; D. Account passwords or personal identification numbers or other access codes; or E. Any of the data elements contained in paragraphs A to D when not in connection with the individual's first name, or first initial, and last name, if the information if compromised	The notices required under paragraphs A and B must be made as expediently as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement pursuant to subsection 3 or with measures necessary to determine the scope of the security breach and restore the reasonable integrity, security and confidentiality of the data in the system. If, after the completion of an investigation required by subsection 1, notification is required under this section, the notification required by this section may be delayed for no longer than 7 business days after a law enforcement agency determines that the notification will not compromise a criminal investigation.	A person that complies with the security breach notification requirements of rules, regulations, procedures or guidelines established pursuant to federal law or the law of this State is deemed to be in compliance with the requirements of section 1348 as long as the law, rules, regulations or guidelines provide for notification procedures at least as protective as the notification requirements of section 1348.	"Notice" means: A. Written notice; B. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 United States Code, Section 7001; or C. Substitute notice, if the person maintaining personal information demonstrates that the cost of providing notice would exceed \$5,000, that the affected class of individuals to be notified exceeds 1,000 or that the person maintaining personal information does not have sufficient contact information to provide written or electronic notice to those individuals. If a person discovers a breach of the security of the system that requires notification to more than 1,000 persons at a single time, the person shall also notify, without unreasonable delay, consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 United States Code, Section 1681a(p). Notification must include the date of the breach, an estimate of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be notified of the breach. When notice of a breach of the security of the system is required under subsection 1, the person	Substitute notice must consist of all of the following: (1) E-mail notice, if the person has e-mail addresses for the individuals to be notified; (2) Conspicuous posting of the notice on the person's publicly accessible website, if the person maintains one; and (3) Notification to major statewide media.	"Breach of the security of the system" or "security breach" means unauthorized acquisition, release or use of an individual's computerized data that includes personal information that compromises the security, confidentiality or integrity of personal information of the individual maintained by a person. Good faith acquisition, release or use of personal information by an employee or agent of a person on behalf of the person is not a breach of the security of the system if the personal information is not used for or subject to further unauthorized disclosure to another person. Information broker. "Information broker" means a person who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>misused and shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur.</p> <p>A 3rd-party entity that maintains, on behalf of a person, computerized data that includes personal information that the 3rd-party entity does not own shall notify the person maintaining personal information of a breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>It is a violation of this chapter for an unauthorized person to release or use an individual's personal information acquired through a security breach.</p>	<p>would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.</p> <p>"Personal information" does not include information from 3rd-party claims databases maintained by property and casualty insurers or publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.</p>			<p>shall notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the person is not regulated by the department, the Attorney General.</p>		<p>information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated 3rd parties. "Information broker" does not include a governmental agency whose records are maintained primarily for traffic safety, law enforcement or licensing purposes.</p>
Maryland	Md. Code, Com. Law § 14-3501 et seq.	A business that owns or licenses computerized data that includes personal information of an individual residing in the State, when it discovers or is notified of a breach of the security of a system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach.	(d)(1) "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 the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable: (i) A Social Security number;	Except as provided in subsection (d) of this section, the notification required under paragraph (2) of this subsection shall be given as soon as reasonably practicable after the business conducts the investigation required under paragraph (1) of this subsection. Prior to giving the	If after the investigation required under paragraph (1) of this subsection is concluded, the business determines that notification under paragraph (2) of this subsection is not required, the business shall maintain records that reflect its determination for 3 years after the determination is made. A business that complies with the requirements for notification procedures, the protection or	The notification required under subsections (b) and (c) of this section may be given: (1) By written notice sent to the most recent address of the individual in the records of the business; (2) By electronic mail to the most recent electronic mail address of the individual in the records of the business, if: (i) The individual has expressly consented to receive electronic notice; or (ii) The business conducts its business primarily through Internet account transactions or the Internet;	Substitute notice under subsection (e)(4) of this section shall consist of: (1) Electronically mailing the notice to an individual entitled to notification under subsection (b) of this section, if the business has an electronic mail address for the individual to be	"Breach of the security of a system" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business; and (2) "Breach of the security of a system" does not include the good faith acquisition of personal information by an employee or agent of a

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/Substitute Notification	Some Definitions
		(2) If after the investigation is concluded, the business determines that misuse of the individual's personal information has occurred or is reasonably likely to occur as a result of a breach of the security of a system, the business shall notify the individual of the breach. A business that maintains computerized data that includes personal information that the business does not own or license shall notify the owner or licensee of the personal information of a breach of the security of a system if it is likely that the breach has resulted or will result in the misuse of personal information of an individual residing in the State. A business that is required to notify an owner or licensee of personal information of a breach of the security of a system under paragraph (1) of this subsection shall share with the owner or licensee information relative to the breach.	(ii) A driver's license number; (iii) A financial account number, including a credit card number or debit card number, that in combination with any required security code, access code, or password, would permit access to an individual's financial account; or (iv) An Individual Taxpayer Identification Number. (2) "Personal information" does not include: (i) Publicly available information that is lawfully made available to the general public from federal, State, or local government records; (ii) Information that an individual has consented to have publicly disseminated or listed; or (iii) Information that is disseminated or listed in accordance with the federal Health Insurance Portability and Accountability Act.	notification required under subsection (b) of this section and subject to subsection (d) of this section, a business shall provide notice of a breach of the security of a system to the Office of the Attorney General. The notification required under subsections (b) and (c) of this section may be delayed: (i) If a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security; or (ii) To determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system. (2) If notification is delayed under paragraph (1)(i) of this subsection, notification shall be given as soon as reasonably practicable after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security.	security of personal information, or the destruction of personal information under the rules, regulations, procedures, or guidelines established by the primary or functional federal or State regulator of the business shall be deemed to be in compliance with this subtitle. A business that is subject to and in compliance with § 501(b) of the federal Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, § 216 of the federal Fair and Accurate Transactions Act, 15 U.S.C. § 1681W, the federal Interagency Guidelines Establishing Information Security Standards, and the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, and any revisions, additions, or substitutions, shall be deemed to be in compliance with this subtitle. An affiliate that complies with § 501(b) of the federal Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, § 216 of the federal Fair and Accurate Transactions Act, 15 U.S.C. § 1681W, the federal Interagency Guidelines Establishing Information Security Standards, and the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, and any revisions, additions, or	(3) By telephonic notice, to the most recent telephone number of the individual in the records of the business; or (4) By substitute notice as provided in subsection (f) of this section, if: (i) The business demonstrates that the cost of providing notice would exceed \$100,000 or that the affected class of individuals to be notified exceeds 175,000; or (ii) The business does not have sufficient contact information to give notice in accordance with item (1), (2), or (3) of this subsection. The notification required under subsection (b) of this section shall include: (1) To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired; (2) Contact information for the business making the notification, including the business' address, telephone number, and toll-free telephone number if one is maintained; (3) The toll-free telephone numbers and addresses for the major consumer reporting agencies; and (4)(i) The toll-free telephone numbers, addresses, and website addresses for: 1. The Federal Trade Commission; and 2. The Office of the Attorney General; and (ii) A statement that an individual can obtain information from these sources about steps the individual can take to avoid identity theft. If a business is required under [this subtitle] to give notice of a breach of the security of a system to 1,000 or more individuals, the business also shall notify, without unreasonable delay, each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a(p), of the timing, distribution,	notified; (2) Conspicuous posting of the notice on the website of the business, if the business maintains a website; and (3) Notification to statewide media.	business for the purposes of the business, provided that the personal information is not used or subject to further unauthorized disclosure.

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
					substitutions, shall be deemed to be in compliance with this subtitle.	and content of the notices. (b) This section does not require the inclusion of the names or other personal identifying information of recipients of notices of the breach of the security of a system.		
Massachusetts	Mass. Gen. Laws § 93H-1 et seq.; 201 CMR 17	The department of consumer affairs and business regulation shall adopt regulations relative to any person that owns or licenses personal information about a resident of the commonwealth. Such regulations shall be designed to safeguard the personal information of residents of the commonwealth and shall be consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated. *** Section 3. (a) A person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the owner or licensor in accordance with this chapter. In addition to providing notice as provided	“Personal information” a resident’s first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver’s license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident’s financial account; provided, however, that “Personal information” shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.	“as soon as practicable and without unreasonable delay” Upon receipt of this notice, the director of consumer affairs and business regulation shall identify any relevant consumer reporting agency or state agency, as deemed appropriate by said director, and forward the names of the identified consumer reporting agencies and state agencies to the notifying person or agency. Such person or agency shall, as soon as practicable and without unreasonable delay, also provide notice, in accordance with this chapter, to the consumer reporting agencies and state agencies identified by the director of consumer affairs and business regulation. Notwithstanding section 3, notice may be delayed if a law enforcement agency determines that provision of such notice may impede a criminal investigation and has notified the attorney general, in writing, thereof and informs the person or	This chapter does not relieve a person or agency from the duty to comply with requirements of any applicable general or special law or federal law regarding the protection and privacy of personal information; provided however, a person who maintains procedures for responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or guidelines, is deemed to be in compliance with this chapter if the person notifies affected Massachusetts residents in accordance with the maintained or required procedures when a breach occurs; provided further that the person also notifies the attorney general and the director of the office of consumer affairs and business regulation of the breach as soon as practicable and without unreasonable delay following the breach. The notice to be provided to the attorney general and the director of the office of consumer affairs and business regulation shall consist of, but not be limited to, any steps the person or agency has taken or plans to take relating to the breach pursuant to the applicable federal law, rule, regulation, guidance or guidelines; provided further that if said person or agency does not comply with applicable federal laws, rules,	“Notice” shall include:— (i) written notice; (ii) electronic notice, if notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 (c) of Title 15 of the United States Code; and chapter 110G; or (iii) substitute notice, if the person or agency required to provide notice demonstrates that the cost of providing written notice will exceed \$250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the person or agency does not have sufficient contact information to provide notice. The notice to be provided to the resident shall include, but not be limited to, the consumer’s right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies, provided however, that said notification shall not include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use.	“Substitute notice”, shall consist of all of the following:— (i) electronic mail notice, if the person or agency has electronic mail addresses for the members of the affected class of Massachusetts residents; (ii) clear and conspicuous posting of the notice on the home page of the person or agency if the person or agency maintains a website; and (iii) publication in or broadcast through media or medium that provides notice throughout the commonwealth.	“Breach of security”, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure. “Encrypted” transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, unless further defined by regulation of the department of consumer affairs and business regulation. The department of

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>herein, such person or agency shall cooperate with the owner or licensor of such information. Such cooperation shall include, but not be limited to, informing the owner or licensor of the breach of security or unauthorized acquisition or use, the date or approximate date of such incident and the nature thereof, and any steps the person or agency has taken or plans to take relating to the incident, except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets, or to provide notice to a resident that may have been affected by the breach of security or unauthorized acquisition or use.</p> <p>(b) A person or agency that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the attorney general, the director of consumer affairs and business regulation and to such resident, in accordance with this chapter.</p>		<p>agency of such determination. If notice is delayed due to such determination and as soon as the law enforcement agency determines and informs the person or agency that notification no longer poses a risk of impeding an investigation, notice shall be provided, as soon as practicable and without unreasonable delay. The person or agency shall cooperate with law enforcement in its investigation of any breach of security or unauthorized acquisition or use, which shall include the sharing of information relevant to the incident; provided however, that such disclosure shall not require the disclosure of confidential business information or trade secrets.</p>	<p>regulations, guidance or guidelines, then it shall be subject to the provisions of this chapter.</p>			<p>consumer affairs and business regulation may adopt regulations, from time to time, to revise the definition of "encrypted", as used in this chapter, to reflect applicable technological advancements.</p> <p>201 CMR 17.00:</p> <p>Breach of security, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.</p> <p>Encrypted, the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		The notice to be provided to the attorney general and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to, the nature of the breach of security or unauthorized acquisition or use, the number of residents of the commonwealth affected by such incident at the time of notification, and any steps the person or agency has taken or plans to take relating to the incident.						“Personal information” shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.
Michigan	Mich. Comp. Laws § 445.63, 445.72	(1) Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach under subsection (2), shall provide a notice of the security breach to each resident of this state who meets 1 or more of the following: (a) That resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person. (b) That resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key. Unless the person or agency	(q) “Personal identifying information” means a name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including, but not limited to, a person's name, address, telephone number, driver license or state personal identification card number, social security number, place of employment number, employer or taxpayer identification number, government passport number, health insurance identification number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or the person's account password, any other account password in combination with sufficient information to identify and	A person or agency shall provide any notice required under this section without unreasonable delay. A person or agency may delay providing notice without violating this subsection if either of the following is met: (a) A delay is necessary in order for the person or agency to take any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database. However, the agency or person shall provide the notice required under this subsection without unreasonable delay after the person or agency completes the measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database.	[The subsection requiring notice to nationwide consumer reporting agencies] does not apply if either of the following is met: (a) The person or agency is required under this section to provide notice of a security breach to 1,000 or fewer residents of this state. (b) The person or agency is subject to 15 USC 6801 to 6809. A financial institution that is subject to, and has notification procedures in place that are subject to examination by the financial institution's appropriate regulator for compliance with, the interagency guidance on response programs for unauthorized access to customer information and customer notice prescribed by the board of governors of the federal reserve system and the other federal bank and thrift regulatory agencies, or similar guidance prescribed and adopted by the national credit union	Except as provided in subsection (11), an agency or person shall provide any notice required under this section by providing 1 or more of the following to the recipient: (a) Written notice sent to the recipient at the recipient's postal address in the records of the agency or person. (b) Written notice sent electronically to the recipient if any of the following are met: (i) The recipient has expressly consented to receive electronic notice. (ii) The person or agency has an existing business relationship with the recipient that includes periodic electronic mail communications and based on those communications the person or agency reasonably believes that it has the recipient's current electronic mail address. (iii) The person or agency conducts its business primarily through internet account transactions or on the internet. (c) If not otherwise prohibited by state or federal law, notice given by telephone by an individual who represents the person or agency if all of the following are met: (i) The notice is not given in whole or in part by use of a recorded message. (ii) The recipient has expressly consented to receive notice by telephone, or if the recipient has	A person or agency provides substitute notice under this subdivision by doing all of the following: (i) If the person or agency has electronic mail addresses for any of the residents of this state who are entitled to receive the notice, providing electronic notice to those residents. (ii) If the person or agency maintains a website, conspicuously posting the notice on that website. (iii) Notifying major statewide media. A notification under this subparagraph shall include a telephone number or a website address that a person may use to obtain	“Breach of the security of a database” or “security breach” means the unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals. These terms do not include unauthorized access to data by an employee or other individual if the access meets all of the following: (i) The employee or other individual acted in good faith in accessing the data. (ii) The access was related to the activities of the agency or person. (iii) The employee or other individual did not misuse any personal information or disclose any personal information to an unauthorized person.

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that maintains a database that includes data that the person or agency does not own or license that discovers a breach of the security of the database shall provide a notice to the owner or licensor of the information of the security breach.</p>	<p>access the account, automated or electronic signature, biometrics, stock or other security certificate or account number, credit card number, vital record, or medical records or information.</p>	<p>(b) A law enforcement agency determines and advises the agency or person that providing a notice will impede a criminal or civil investigation or jeopardize homeland or national security. However, the agency or person shall provide the notice required under this section without unreasonable delay after the law enforcement agency determines that providing the notice will no longer impede the investigation or jeopardize homeland or national security.</p>	<p>administration, and its affiliates, is considered to be in compliance with this section.</p> <p>A person or agency that is subject to and complies with the health insurance portability and accountability act of 1996, Public Law 104-191, and with regulations promulgated under that act, 45 CFR parts 160 and 164, for the prevention of unauthorized access to customer information and customer notice is considered to be in compliance with this section.</p>	<p>not expressly consented to receive notice by telephone, the person or agency also provides notice under subdivision (a) or (b) if the notice by telephone does not result in a live conversation between the individual representing the person or agency and the recipient within 3 business days after the initial attempt to provide telephonic notice.</p> <p>(d) Substitute notice, if the person or agency demonstrates that the cost of providing notice under subdivision (a), (b), or (c) will exceed \$250,000.00 or that the person or agency has to provide notice to more than 500,000 residents of this state.</p> <p>A notice under this section shall do all of the following:</p> <p>(a) For a notice provided under subsection (5)(a) or (b), be written in a clear and conspicuous manner and contain the content required under subdivisions (c) to (g).</p> <p>(b) For a notice provided under subsection (5)(c), clearly communicate the content required under subdivisions (c) to (g) to the recipient of the telephone call.</p> <p>(c) Describe the security breach in general terms.</p> <p>(d) Describe the type of personal information that is the subject of the unauthorized access or use.</p> <p>(e) If applicable, generally describe what the agency or person providing the notice has done to protect data from further security breaches.</p> <p>(f) Include a telephone number where a notice recipient may obtain assistance or additional information.</p> <p>(g) Remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft.</p> <p>Except as provided in this subsection, after a person or agency provides a notice under this section, the person or agency shall notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the</p>	<p>additional assistance and information.</p>	<p>(g) "Encrypted" means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing information by another method that renders the data elements unreadable or unusable.</p> <p>(i) "Financial institution" means a depository institution, an affiliate of a depository institution, a licensee under the consumer financial services act, 1988 PA 161, MCL 487.2051 to 487.2072, 1984 PA 379, MCL 493.101 to 493.114, the motor vehicle sales finance act, 1950 (Ex Sess) PA 27, MCL 492.101 to 492.141, the secondary mortgage loan act, 1981 PA 125, MCL 493.51 to 493.81, the mortgage brokers, lenders, and servicers licensing act, 1987 PA 173, MCL 445.1651 to 445.1684, or the regulatory loan act, 1939 PA 21, MCL 493.1 to 493.24, a seller under the home improvement finance act, 1965 PA 332, MCL 445.1101 to 445.1431, or the retail installment sales act, 1966 PA 224, MCL 445.851 to 445.873, or a person subject to subtitle A of title V of the Gramm-Leach-Bliley act, 15 USC 6801 to 6809.</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
						<p>security breach without unreasonable delay. A notification under this subsection shall include the number of notices that the person or agency provided to residents of this state and the timing of those notices.</p> <p>A public utility that sends monthly billing or account statements to the postal address of its customers may provide notice of a security breach to its customers in the manner described in subsection (5), or alternatively by providing all of the following:</p> <p>(a) As applicable, notice as described in subsection (5)(b).</p> <p>(b) Notification to the media reasonably calculated to inform the customers of the public utility of the security breach.</p> <p>(c) Conspicuous posting of the notice of the security breach on the website of the public utility.</p> <p>(d) Written notice sent in conjunction with the monthly billing or account statement to the customer at the customer's postal address in the records of the public utility.</p>		
Minnesota	Minn. Stat. §§ 325E.61 [data warehouses], 325E.64 [access devices]; 13.055 [state agencies]	(a) Any person or business that conducts business in this state, and that owns or licenses 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 this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in paragraph (c), or with	For purposes of this section and section 13.055, subdivision 6, "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 the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired:	The notification required by this section and section 13.055, subdivision 6, may be delayed to a date certain if a law enforcement agency affirmatively determines that the notification will impede a criminal investigation.	This section and section 13.055, subdivision 6, do not apply to any "financial institution" as defined by United States Code, title 15, section 6809(3).	For purposes of this section and section 13.055, subdivision 6, "notice" may be provided by one of the following methods:	Substitute notice must consist of all of the following:	325E..61: For purposes of this section and section 13.055, subdivision 6, "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 system, provided that the personal

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.</p> <p>(b) Any person or business that maintains 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.</p>	<p>(2) driver's license number or Minnesota identification card number; or</p> <p>(3) account number or 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.</p> <p>"personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.</p>			<p>Notwithstanding paragraph (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 section and section 13.055, subdivision 6, shall be deemed to be in compliance with the notification requirements of this section and section 13.055, subdivision 6, if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.</p> <p>If a person discovers circumstances requiring notification under this section and section 13.055, subdivision 6, of more than 500 persons at one time, the person shall also notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by United States Code, title 15, section 1681a, of the timing, distribution, and content of the notices.</p>	<p>media.</p>	<p>information is not used or subject to further unauthorized disclosure.</p> <p>325E.64:</p> <p>"Access device" means a card issued by a financial institution that contains a magnetic stripe, microprocessor chip, or other means for storage of information which includes, but is not limited to, a credit card, debit card, or stored value card.</p>
Mississippi	Miss. Code § 75-24-29	<p>A person who conducts business in this state shall disclose any breach of security to all affected individuals.</p> <p>Any person who conducts business in this state that maintains computerized data which includes personal information that the person does not own or license shall notify the owner or licensee of the information of any breach of the security of the data as soon as practicable following its discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person for</p>	<p>"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:</p> <p>(i) Social security number;</p> <p>(ii) Driver's license number or state identification card number; or</p> <p>(iii) An account number or 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; "personal information" does not include publicly available information</p>	<p>The disclosure shall be made without unreasonable delay, subject to the provisions of subsections (4) and (5) of this section and the completion of an investigation by the person to determine the nature and scope of the incident, to identify the affected individuals, or to restore the reasonable integrity of the data system.</p> <p>Any notification required by this section shall be delayed for a reasonable period of time if a law enforcement agency determines that the</p>	<p>Notification shall not be required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals.</p> <p>Any person who conducts business in this state that maintains its own security breach procedures as part of an information security policy for the treatment of personal information, and otherwise complies with the timing requirements of this section, shall be deemed to be in compliance with the security breach notification requirements of this section if the person notifies affected individuals in accordance</p>	<p>Any notice required by the provisions of this section may be provided by one (1) of the following methods: (a) written notice; (b) telephone notice; (c) electronic notice, if the person's primary means of communication with the affected individuals is by electronic means or if the notice is consistent with the provisions regarding electronic records and signatures set forth in 15 USC § 7001; or (d) substitute notice, provided the person demonstrates that the cost of providing notice in accordance with paragraph (a), (b) or (c) of this subsection would exceed Five Thousand Dollars (\$5,000.00), that the affected class of subject persons to be notified exceeds five thousand (5,000) individuals or the person does not have sufficient contact information.</p>	<p>Substitute notice shall consist of the following: electronic mail notice when the person has an electronic mail address for the affected individuals; conspicuous posting of the notice on the Web site of the person if the person maintains one; and notification to major statewide media, including newspapers, radio and television.</p>	<p>"Breach of security" means unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of this state when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable;</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		fraudulent purposes.	that is lawfully made available to the general public from federal, state or local government records or widely distributed media;	notification will impede a criminal investigation or national security and the law enforcement agency has made a request that the notification be delayed. Any such delayed notification shall be made after the law enforcement agency determines that notification will not compromise the criminal investigation or national security and so notifies the person of that determination.	with the person's policies in the event of a breach of security. Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or federal functional regulator, as defined in 15 USC § 6809(2), shall be deemed to be in compliance with the security breach notification requirements of this section, provided the person notifies affected individuals in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or federal functional regulator in the event of a breach of security of the system.			
Missouri	Mo. Rev. Stat. § 407.1500	Any person that owns or licenses personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri shall provide notice to the affected consumer that there has been a breach of security following discovery or notification of the breach. The disclosure notification shall be: (a) Made without unreasonable delay; (b) Consistent with the legitimate needs of law enforcement, as provided in this section; and (c) Consistent with any measures necessary to determine sufficient contact information and to determine the scope of the breach and restore the	“Personal information”, an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable: (a) Social Security number; (b) Driver's license number or other unique identification number created or collected by a government body; (c) Financial account number, credit card number, or debit card number in combination with any required security	“without unreasonable delay” The notice required by this section may be delayed if a law enforcement agency informs the person that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request by law enforcement is made in writing or the person documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the	Notwithstanding subdivisions (1) and (2) of this subsection, notification is not required if, after an appropriate investigation by the person or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach. Such a determination shall be documented in writing and the documentation shall be maintained for five years. A person that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are	The notice shall at minimum include a description of the following: (a) The incident in general terms; (b) The type of personal information that was obtained as a result of the breach of security; (c) A telephone number that the affected consumer may call for further information and assistance, if one exists; (d) Contact information for consumer reporting agencies; (e) Advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports. For purposes of this section, notice to affected consumers shall be provided by one of the following methods: (a) Written notice; (b) Electronic notice for those consumers for whom the person has a valid e-mail address and who have agreed to receive communications electronically, if the notice provided is consistent	Substitute notice under paragraph (d) of subdivision (6) of this subsection shall consist of all the following: (a) E-mail notice when the person has an electronic mail address for the affected consumer; (b) Conspicuous posting of the notice or a link to the notice on the Internet web site of the person if the person maintains an Internet website; and (c) Notification to major statewide media.	“Breach of security” or “breach”, unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>reasonable integrity, security, and confidentiality of the data system.</p> <p>Any person that maintains or possesses records or data containing personal information of residents of Missouri that the person does not own or license, or any person that conducts business in Missouri that maintains or possesses records or data containing personal information of a resident of Missouri that the person does not own or license, shall notify the owner or licensee of the information of any breach of security immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in this section.</p>	<p>code, access code, or password that would permit access to an individual's financial account;</p> <p>(d) Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account;</p> <p>(e) Medical information; or</p> <p>(f) Health insurance information.</p> <p>"Personal information" does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public;</p>	<p>investigation. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicates to the person its determination that notice will no longer impede the investigation or jeopardize national or homeland security.</p>	<p>otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section if the person notifies affected consumers in accordance with its policies in the event of a breach of security of the system.</p> <p>A person that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section if the person notifies affected consumers in accordance with the maintained procedures when a breach occurs.</p> <p>A financial institution that is:</p> <p>(a) Subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued on March 29, 2005, by the board of governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to said interagency guidance; or</p> <p>(b) Subject to and in compliance with the National Credit Union Administration regulations in 12 CFR Part 748; or</p>	<p>with the provisions of 15 U.S.C. Section 7001 regarding electronic records and signatures for notices legally required to be in writing;</p> <p>(c) Telephonic notice, if such contact is made directly with the affected consumers; or</p> <p>(d) Substitute notice, if:</p> <p>a. The person demonstrates that the cost of providing notice would exceed one hundred thousand dollars; or</p> <p>b. The class of affected consumers to be notified exceeds one hundred fifty thousand; or</p> <p>c. The person does not have sufficient contact information or consent to satisfy paragraphs (a), (b), or (c) of this subdivision, for only those affected consumers without sufficient contact information or consent; or</p> <p>d. The person is unable to identify particular affected consumers, for only those unidentifiable consumers.</p> <p>In the event a person provides notice to more than one thousand consumers at one time pursuant to this section, the person shall notify, without unreasonable delay, the attorney general's office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. Section 1681a(p), of the timing, distribution, and content of the notice.</p>		<p>information;</p> <p>"Encryption", the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key;</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
					(c) Subject to and in compliance with the provisions of Title V of the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. Sections 6801 to 6809; shall be deemed to be in compliance with this section.			
Montana	Mont. Code §§ 30-14-1704 [commercial entity], 2-6-504 [state agency]	<p>Any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the data system following discovery or notification of the breach to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.</p> <p>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 system immediately following discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person.</p>	<p>"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:</p> <p>(A) social security number; (B) driver's license number, state identification card number, or tribal identification card number; (C) account number or 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.</p> <p>(ii) Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.</p>	<p>The disclosure must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3), or consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.</p> <p>The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and requests a delay in notification. The notification required by this section must be made after the law enforcement agency determines that it will not compromise the investigation.</p>	<p>Notwithstanding subsection (5), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and that does not unreasonably delay notice is considered 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 data system.</p>	<p>For purposes of this section, notice may be provided by one of the following methods:</p> <p>(i) written notice; (ii) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001; (iii) telephonic notice; or (iv) substitute notice, if the person or business demonstrates that:</p> <p>(A) the cost of providing notice would exceed \$250,000; (B) the affected class of subject persons to be notified exceeds 500,000; or (C) the person or business does not have sufficient contact information.</p> <p>If a business discloses a security breach to any individual pursuant to this section and gives a notice to the individual that suggests, indicates, or implies to the individual that the individual may obtain a copy of the file on the individual from a consumer credit reporting agency, the business shall coordinate with the consumer reporting agency as to the timing, content, and distribution of the notice to the individual. The coordination may not unreasonably delay the notice to the affected individuals.</p>	<p>Substitute notice must consist of the following:</p> <p>(i) an electronic mail notice when the person or business has an electronic mail address for the subject persons; and (ii) conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; or (iii) notification to applicable local or statewide media.</p>	<p>"Breach of the security of the data system" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident. 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 data system, provided that the personal information is not used or subject to further unauthorized disclosure.</p>
Nebraska	Neb. Rev. Stat. §§ 87-801-807	An individual or a commercial entity that conducts business in Nebraska and that owns or licenses computerized data that includes personal information about a resident of Nebraska shall, when it becomes aware of a breach of the security of the	Personal information means a Nebraska resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident if either the name or the data elements are not	If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the individual or commercial entity shall	An individual or a commercial entity that maintains its own notice procedures which are part of an information security policy for the treatment of personal information and which are otherwise consistent with the timing requirements of section 87-803, is deemed to be in	<p>Notice means:</p> <p>(a) Written notice; (b) Telephonic notice; (c) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001, as such section existed on January 1, 2006; (d) Substitute notice, if the individual or commercial</p>	<p>Substitute notice [for larger breaches] requires all of the following:</p> <p>(i) Electronic mail notice if the individual or commercial entity has electronic mail</p>	<p>Breach of the security of the system means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be used for an unauthorized purpose.</p> <p>An individual or a commercial entity that maintains computerized data that includes personal information that the individual or commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system when it becomes aware of a breach if use of personal information about a Nebraska resident for an unauthorized purpose occurred or is reasonably likely to occur. Cooperation includes, but is not limited to, sharing with the owner or licensee information relevant to the breach, not including information proprietary to the individual or commercial entity.</p>	<p>encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable:</p> <p>(a) Social security number;</p> <p>(b) Motor vehicle operator's license number or state identification card number;</p> <p>(c) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account;</p> <p>(d) Unique electronic identification number or routing code, in combination with any required security code, access code, or password; or</p> <p>(e) Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation.</p> <p>Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records</p>	<p>give notice to the affected Nebraska resident. Notice shall be made as soon as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.</p> <p>Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice shall be made in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.</p>	<p>compliance with the notice requirements of section 87-803 if the individual or the commercial entity notifies affected Nebraska residents in accordance with its notice procedures in the event of a breach of the security of the system.</p> <p>An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with section 87-803 if the individual or commercial entity notifies affected Nebraska residents in accordance with the maintained procedures in the event of a breach of the security of the system.</p>	<p>entity required to provide notice demonstrates that the cost of providing notice will exceed seventy-five thousand dollars, that the affected class of Nebraska residents to be notified exceeds one hundred thousand residents, or that the individual or commercial entity does not have sufficient contact information to provide notice.</p> <p>(e) Substitute notice, if the individual or commercial entity required to provide notice has ten employees or fewer and demonstrates that the cost of providing notice will exceed ten thousand dollars.</p>	<p>addresses for the members of the affected class of Nebraska residents;</p> <p>(ii) Conspicuous posting of the notice on the web site of the individual or commercial entity if the individual or commercial entity maintains a web site; and</p> <p>(iii) Notice to major statewide media outlets;</p> <p>Substitute notice [for small employers] requires all of the following:</p> <p>(i) Electronic mail notice if the individual or commercial entity has electronic mail addresses for the members of the affected class of Nebraska residents;</p> <p>(ii) Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the individual or commercial entity is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and</p>	<p>individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system if the personal information is not used or subject to further unauthorized disclosure. Acquisition of personal information pursuant to a search warrant, subpoena, or other court order or pursuant to a subpoena or order of a state agency is not a breach of the security of the system;</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
							shall be published in the newspaper at least once a week for three consecutive weeks; (iii) Conspicuous posting of the notice on the web site of the individual or commercial entity if the individual or commercial entity maintains a web site; and (iv) Notification to major media outlets in the geographic area in which the individual or commercial entity is located;	
Nevada	Nev. Rev. Stat. §§ 603A.010 et seq. [commercial entities]; 242.183 [state agencies]	Any data collector that owns or licenses computerized data which includes personal information shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Any data collector that maintains computerized data which includes personal information that the data collector does not own shall notify the owner or licensee of the information of any breach of the security of the system data immediately following discovery if the personal information was, or is	“Personal information” means a natural person’s first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted: 1. Social security number. 2. Driver’s license number or identification card number. 3. Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person’s financial account. The term does not include the last four digits of a social security number, the last four digits of a driver’s license	The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection 3, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data. 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 must be made after the law enforcement agency	The provisions of this chapter do not apply to the maintenance or transmittal of information in accordance with NRS 439.581 to 439.595, inclusive, and the regulations adopted pursuant thereto. A data collector which: (a) Maintains its own notification policies and procedures as part of an information security policy for the treatment of personal information that is otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if the data collector notifies subject persons in accordance with its policies and procedures in the event of a breach of the security of the	For purposes of this section, except as otherwise provided in subsection 5, the notification required by this section may be provided by one of the following methods: (a) Written notification. (b) Electronic notification, if the notification provided is consistent with the provisions of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001 et seq. (c) Substitute notification, if the data collector demonstrates that the cost of providing notification would exceed \$250,000, the affected class of subject persons to be notified exceeds 500,000 or the data collector does not have sufficient contact information. If a data collector determines that notification is required to be given pursuant to the provisions of this section to more than 1,000 persons at any one time, the data collector shall also notify, without unreasonable delay, any consumer reporting agency, as that term is defined in 15 U.S.C. § 1681a(p), that compiles and maintains files on	Substitute notification must consist of all the following: (1) Notification by electronic mail when the data collector has electronic mail addresses for the subject persons. (2) Conspicuous posting of the notification on the Internet website of the data collector, if the data collector maintains an Internet website. (3) Notification to major statewide media.	“Breach of the security of the system data” defined. “Breach of the security of the system data” means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector. The term does not include the good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, so long as the personal information is not used for a purpose unrelated to the data collector or subject to further unauthorized disclosure.

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		reasonably believed to have been, acquired by an unauthorized person.	number or the last four digits of an identification card number or publicly available information that is lawfully made available to the general public.	determines that the notification will not compromise the investigation.	system data. (b) Is subject to and complies with the privacy and security provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et seq., shall be deemed to be in compliance with the notification requirements of this section.	consumers on a nationwide basis, of the time the notification is distributed and the content of the notification.		(b) "Encryption" means the protection of data in electronic or optical form, in storage or in transit, using: (1) An encryption technology that has been adopted by an established standards setting body, including, but not limited to, the Federal Information Processing Standards issued by the National Institute of Standards and Technology, which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; (2) Appropriate management and safeguards of cryptographic keys to protect the integrity of the encryption using guidelines promulgated by an established standards setting body, including, but not limited to, the National Institute of Standards and Technology; and (3) Any other technology or method identified by the Division of Enterprise Information Technology Services of the Department of Administration in regulations adopted pursuant to NRS 603A.217.
New Hampshire	N.H. Rev. Stat. §§ 359-C:19-21	Any person doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has	(a) "Personal information" means an individual's first name or 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	The disclosure shall be made to affected individuals as quickly as possible, after the determination required under this section. Notification pursuant to	Any person engaged in trade or commerce that is subject to RSA 358-A:3, I which maintains procedures for security breach notification pursuant to the laws, rules, regulations, guidances, or guidelines issued by a state or	Any person engaged in trade or commerce that is subject to RSA 358-A:3, I shall also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the New Hampshire attorney general's office. The notice shall include the anticipated date of the notice to the individuals and the approximate	Substitute notice shall consist of all of the following: (1) E-mail notice when the person has an e-mail address for the affected	"Encrypted" means the transformation of data through the use of an algorithmic process into a form for which there is a low probability of assigning meaning without use of a confidential process or

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible as required under this subdivision.</p> <p>Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify and cooperate with the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was acquired by an unauthorized person. Cooperation includes sharing with the owner or licensee information relevant to the breach; except that such cooperation shall not be deemed to require the disclosure of confidential or business information or trade secrets.</p>	<p>not encrypted:</p> <p>(1) Social security number.</p> <p>(2) Driver's license number or other government identification number.</p> <p>(3) Account number, credit card number, 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.</p> <p>(b) "Personal information" shall not include information that is lawfully made available to the general public from federal, state, or local government records.</p>	<p>paragraph I may be delayed if a law enforcement agency, or national or homeland security agency determines that the notification will impede a criminal investigation or jeopardize national or homeland security.</p>	<p>federal regulator shall be deemed to be in compliance with this subdivision if it acts in accordance with such laws, rules, regulations, guidances, or guidelines.</p> <p>(a) If a person is required to notify more than 1,000 consumers of a breach of security pursuant to this section, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. section 1681a(p), of the anticipated date of the notification to the consumers, the approximate number of consumers who will be notified, and the content of the notice. Nothing in this paragraph shall be construed to require the person to provide to any consumer reporting agency the names of the consumers entitled to receive the notice or any personal information relating to them.</p> <p>(b) Subparagraph (a) shall not apply to a person who is subject to Title V of the Gramm, Leach-Bliley Act, 15 U.S.C. section 6801 et seq.</p>	<p>number of individuals in this state who will be notified. Nothing in this section shall be construed to require the person to provide to any regulator or the New Hampshire attorney general's office the names of the individuals entitled to receive the notice or any personal information relating to them.</p> <p>The notice required under this section shall be provided by one of the following methods:</p> <p>(a) Written notice.</p> <p>(b) Electronic notice, if the agency or business' primary means of communication with affected individuals is by electronic means.</p> <p>(c) Telephonic notice, provided that a log of each such notification is kept by the person or business who notifies affected persons.</p> <p>(d) Substitute notice, if the person demonstrates that the cost of providing notice would exceed \$5,000, that the affected class of subject individuals to be notified exceeds 1,000, or the person does not have sufficient contact information or consent to provide notice pursuant to subparagraphs I(a)-I(c). ***</p> <p>(e) Notice pursuant to the person's internal notification procedures maintained as part of an information security policy for the treatment of personal information.</p> <p>Notice under this section shall include at a minimum:</p> <p>(a) A description of the incident in general terms.</p> <p>(b) The approximate date of breach.</p> <p>(c) The type of personal information obtained as a result of the security breach.</p> <p>(d) The telephonic contact information of the person subject to this section.</p>	<p>individuals.</p> <p>(2) Conspicuous posting of the notice on the person's business website, if the person maintains one.</p> <p>(3) Notification to major statewide media.</p>	<p>key, or securing the information by another method that renders the data elements completely unreadable or unusable. Data shall not be considered to be encrypted for purposes of this subdivision if it is acquired in combination with any required key, security code, access code, or password that would permit access to the encrypted data.</p> <p>"Security breach" means unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state. Good faith acquisition of personal information by an employee or agent of a person for the purposes of the person's business shall not be considered a security breach, provided that the personal information is not used or subject to further unauthorized disclosure.</p>
New Jersey	N.J. Stat. 56:8-161-166	Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of	"Personal information" means an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2)	The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the	Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any	Any business or public entity required under this section to disclose a breach of security of a customer's personal information shall, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the	Substitute notice shall consist of all of the following: (a) E-mail notice when the business or public entity has an e-mail	"Breach of security" means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person.</p> <p>Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers, as provided in subsection a. of this section, of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.</p>	<p>driver's license number or State identification card number; or (3) account number or 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.</p> <p>Dissociated data that, if linked, would constitute personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.</p> <p>personal information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media.</p>	<p>legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.</p> <p>The notification required by this section shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies that business or public entity.</p>	<p>determination shall be documented in writing and retained for five years.</p> <p>Notwithstanding subsection d. of this section, a business or public entity 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 requirements of this section, shall be deemed to be in compliance with the notification requirements of this section if the business or public entity notifies subject customers in accordance with its policies in the event of a breach of security of the system.</p>	<p>Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities.</p> <p>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 101 of the federal "Electronic Signatures in Global and National Commerce Act" (15 U.S.C. s.7001); or (3) Substitute notice, if the business or public entity demonstrates that the cost of providing notice would exceed \$250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the business or public entity does not have sufficient contact information.</p> <p>In addition to any other disclosure or notification required under this section, in the event that a business or public entity discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at one time, the business or public entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis, as defined by subsection (p) of section 603 of the federal "Fair Credit Reporting Act" (15 U.S.C. s. 1681a), of the timing, distribution and content of the notices.</p>	<p>address; (b) Conspicuous posting of the notice on the Internet web site page of the business or public entity, if the business or public entity maintains one; and (c) Notification to major Statewide media.</p>	<p>integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Good faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.</p> <p>"Communicate" means to send a written or other tangible record or to transmit a record by any means agreed upon by the persons sending and receiving the record.</p> <p>"Records" means any material, regardless of the physical form, on which information is recorded or preserved by any means, including written or spoken words, graphically depicted, printed, or electromagnetically transmitted. Records does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed.</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
New Mexico	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION
New York	N.Y. Gen. Bus. Law § 899-aa	<p>Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.</p> <p>Any person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.</p>	<p>(a) "Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;</p> <p>(b) "Private information" shall mean personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired:</p> <p>(1) social security number;</p> <p>(2) driver's license number or non-driver identification card number;</p> <p>or</p> <p>(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;</p> <p>"Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.</p>	<p>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 four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.</p> <p>The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.</p>	<p><i>No exception to notification noted in the statute</i></p>	<p>The notice required by this section shall be directly provided to the affected persons by one of the following methods:</p> <p>(a) written notice;</p> <p>(b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction.</p> <p>(c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or</p> <p>(d) Substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information.</p> <p>Regardless of the method by which notice is provided, such notice shall include contact information for the person or business making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.</p> <p>In the event that any New York residents are to be notified, the person or business shall notify the state attorney general, the department of state and the state office of cyber security and critical</p>	<p>Substitute notice shall consist of all of the following:</p> <p>(1) e-mail notice when such business has an e-mail address for the subject persons;</p> <p>(2) conspicuous posting of the notice on such business's web site page, if such business maintains one; and</p> <p>(3) notification to major statewide media.</p>	<p>"Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. Good faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.</p> <p>In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others:</p> <p>(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or</p> <p>(2) indications that the information has been downloaded or copied; or</p> <p>(3) indications that the information was used by an</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
						<p>infrastructure coordination as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.</p> <p>(b) In the event that more than five thousand New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.</p>		<p>unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.</p>
North Carolina	N.C. Gen. Stat §§ 75-61 [definitions], 75-65	<p>Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach.</p> <p>Any business that maintains or possesses records or data containing personal information of residents of North Carolina that the business does not own or license, or any business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach,</p>	<p>“Personal information”. -- A person’s first name or first initial and last name in combination with identifying information as defined in G.S. 14-113.20(b). Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records.</p> <p>For the purposes of this section, personal information shall not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent’s legal surname prior to marriage, or a</p>	<p>The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this section, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.</p> <p>The notice required by this section shall be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the business documents such request contemporaneously in</p>	<p>A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision; or a credit union that is subject to and in compliance with the Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration; and any revisions, additions, or substitutions relating to any of the said interagency guidance, shall be deemed to be in compliance with this section.</p>	<p>The notice shall be clear and conspicuous. The notice shall include all of the following:</p> <ol style="list-style-type: none"> (1) A description of the incident in general terms. (2) A description of the type of personal information that was subject to the unauthorized access and acquisition. (3) A description of the general acts of the business to protect the personal information from further unauthorized access. (4) A telephone number for the business that the person may call for further information and assistance, if one exists. (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. (6) The toll-free numbers and addresses for the major consumer reporting agencies. (7) The toll-free numbers, addresses, and Web site addresses for the Federal Trade Commission and the North Carolina Attorney General’s Office, along with a statement that the individual can obtain information from these sources about preventing identity theft. <p>For purposes of this section, notice to affected persons may be provided by one of the following methods:</p> <ol style="list-style-type: none"> (1) Written notice. 	<p>Substitute notice shall consist of all the following:</p> <ol style="list-style-type: none"> a. E-mail notice when the business has an electronic mail address for the subject persons. b. Conspicuous posting of the notice on the Web site page of the business, if one is maintained. c. Notification to major statewide media. 	<p>“Records”. -- Any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.</p> <p>“Redaction”. -- The rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number is accessible as part of the data.</p> <p>“Security breach”. -- An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section.	password unless this information would permit access to a person's financial account or resources.	writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicates to the business its determination that notice will no longer impede the investigation or jeopardize national or homeland security.		(2) Electronic notice, for those persons for whom it has a valid e-mail address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001. (3) Telephonic notice provided that contact is made directly with the affected persons. (4) Substitute notice, if the 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 if the business does not have sufficient contact information or consent to satisfy subdivisions (1), (2), or (3) of this subsection, for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. (e1) In the event a business provides notice to an affected person pursuant to this section, the business shall notify without unreasonable delay the Consumer Protection Division of the Attorney General's Office of the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice. (f) In the event a business provides notice to more than 1,000 persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice.		confidential process or key shall constitute a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.
North Dakota	N.D. Cent. Code § 51-30-	Any person that conducts business in this state, and that	"Personal information" means an individual's first name or	The disclosure must be made in the most expedient	Notwithstanding section 51-30-05, a person that maintains its own	Notice under this chapter may be provided by one of the following methods:	Substitute notice consists of the	"Breach of the security system" [sic] means

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
	01 et seq.	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 the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following the discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted: (1) The individual's social security number; (2) The operator's license number assigned to an individual by the department of transportation under section 39-06-14; (3) A nondriver color photo identification card number assigned to the individual by the department of transportation under section 39-06-03.1; (4) The individual's financial institution account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts; (5) The individual's date of birth; (6) The maiden name of the individual's mother; (7) An identification number assigned to the individual by the individual's employer; or (8) The individual's digitized or other electronic signature. b. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.	time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in section 51-30-04, or any measures necessary to determine the scope of the breach and to restore the integrity of the data system. The notification required by this chapter may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this chapter must be made after the law enforcement agency determines that the notification will not compromise the investigation.	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 chapter is deemed to be in compliance with the notification requirements of this chapter if the person notifies subject individuals in accordance with its policies in the event of a breach of security of the system. A financial institution, trust company, or credit union that is subject to, examined for, and in compliance with the federal interagency guidance on response programs for unauthorized access to customer information and customer notice is deemed to be in compliance with this chapter.	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; or 3. Substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person does not have sufficient contact information.	following: a. E-mail notice when the person has an e-mail address for the subject persons; b. Conspicuous posting of the notice on the person's website page, if the person maintains one; and c. Notification to major statewide media.	unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable. Good-faith acquisition of personal information by an employee or agent of the person is not a breach of the security of the system, if the personal information is not used or subject to further unauthorized disclosure.

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
Ohio	Ohio Rev. Code §§ 1347.12 [state agencies], 1349.19-.192	(B)(1) Any person that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. The disclosure described in this division may be made pursuant to any provision of a contract entered into by the person with another person prior to the date the breach of the security of the system occurred if that contract does not conflict with any provision of this section and does not waive any provision of this section. For purposes of this section, a resident of this state is an individual whose principal mailing address as reflected in the records of the person is in this state. Any person that, on behalf of or at the direction of another person or on behalf of or at the direction of any governmental entity, is the custodian of or stores computerized data that includes personal information shall notify that other person or	“Personal information” means an individual’s name, consisting of the individual’s first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: (i) Social security number; (ii) Driver’s license number or state identification card number; (iii) Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual’s financial account. (b) “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or any of the following media that are widely distributed: (i) Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television; (ii) Any gathering or furnishing of information or news by any bona fide reporter,	The person shall make the disclosure described in division (B)(1) of this section in the most expedient time possible but not later than forty-five days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities described in division (D) of this section and consistent with any measures necessary to determine the scope of the breach, including which residents’ personal information was accessed and acquired, and to restore the reasonable integrity of the data system. The person may delay the disclosure or notification required by division (B), (C), or (G) of this section if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security, in which case, the person shall make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation or jeopardize homeland or national	(F)(1) A financial institution, trust company, or credit union or any affiliate of a financial institution, trust company, or credit union that is required by federal law, including, but not limited to, any federal statute, regulation, regulatory guidance, or other regulatory action, to notify its customers of an information security breach with respect to information about those customers and that is subject to examination by its functional government regulatory agency for compliance with the applicable federal law, is exempt from the requirements of this section. (2) This section does not apply to any person or entity that is a covered entity as defined in 45 C.F.R. 160.103, as amended.	For purposes of this section, a person may disclose or make a notification by any of the following methods: (1) Written notice; (2) Electronic notice, if the person’s primary method of communication with the resident to whom the disclosure must be made is by electronic means; (3) Telephone notice; (4) Substitute notice in accordance with this division, if the person required to disclose demonstrates that the person does not have sufficient contact information to provide notice in a manner described in division (E)(1), (2), or (3) of this section, or that the cost of providing disclosure or notice to residents to whom disclosure or notification is required would exceed two hundred fifty thousand dollars, or that the affected class of subject residents to whom disclosure or notification is required exceeds five hundred thousand persons. If a person discovers circumstances that require disclosure under this section to more than one thousand residents of this state involved in a single occurrence of a breach of the security of the system, the person shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given by the person to the residents of this state. In no case shall a person that is required to make a notification required by this division delay any disclosure or notification required by division (B) or (C) of this section in order to make the notification required by this division.	Substitute notice under this division shall consist of all of the following: (a) Electronic mail notice if the person has an electronic mail address for the resident to whom the disclosure must be made; (b) Conspicuous posting of the disclosure or notice on the person’s web site, if the person maintains one; (c) Notification to major media outlets, to the extent that the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equals or exceeds seventy-five per cent of the population of this state. (5) Substitute notice in accordance with this division, if the person required to disclose demonstrates that the person is a business entity with ten employees or fewer and that the cost of providing the disclosures or notices to residents to whom disclosure or	“Breach of the security of the system” means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state. For purposes of division (A)(1)(a) of this section: (i) Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security of the system, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure. (ii) Acquisition of personal information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency, is not a breach of the security of the system. “System” means any collection or group of related records that are kept in an organized manner, that are maintained by a person, and from which personal information is

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		governmental entity of any breach of the security of the system in an expeditious manner, if the personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of this state.	correspondent, or news bureau to news media described in division (A)(7)(b)(i) of this section; (iii) Any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation; (iv) Any type of media similar in nature to any item, entity, or activity identified in division (A)(7)(b)(i), (ii), or (iii) of this section.	security.			notification is required will exceed ten thousand dollars. Substitute notice under this division shall consist of all of the following: (a) Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the business entity is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks; (b) Conspicuous posting of the disclosure or notice on the business entity's web site, if the entity maintains one; (c) Notification to major media outlets in the geographic area in which the business entity is located.	retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. "System" does not include any published directory, any reference material or newsletter, or any routine information that is maintained for the purpose of internal office administration of the person, if the use of the directory, material, newsletter, or information would not adversely affect an individual, and there has been no unauthorized external breach of the directory, material, newsletter, or information.
Oklahoma	Okla. Stat. § 74-3113.1 [state agencies]; § 24-161 to -166	An individual or entity 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 of the security of the system to any	"Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor	Except as provided in subsection D of this section [law enforcement delay] or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the	An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of this act [FN1] shall be deemed to be in compliance with the notification	"Notice" means: a. written notice to the postal address in the records of the individual or entity, b. telephone notice, c. electronic notice, or d. substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed Fifty Thousand	Substitute notice consists of any two of the following: (1) e-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of	"Breach of the security of a system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>resident of this state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state.</p> <p>An individual or entity must disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of this state.</p> <p>C. An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery, if the personal information was or if the entity reasonably believes was accessed and acquired by an unauthorized person.</p>	<p>redacted:</p> <p>a. social security number, b. driver license number or state identification card number issued in lieu of a driver license, or c. financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to the financial accounts of a resident.</p> <p>The term does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public;</p>	<p>system, the disclosure shall be made without unreasonable delay.</p> <p>Notice required by this section may be delayed if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation or homeland or national security. Notice required by this section must be made without unreasonable delay after the law enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security.</p>	<p>requirements of this act if it notifies residents of this state in accordance with its procedures in the event of a breach of security of the system.</p> <p>B. 1. A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with the provisions of this act.</p> <p>2. An entity that complies with the notification requirements or procedures pursuant to the rules, regulation, procedures, or guidelines established by the primary or functional federal regulator of the entity shall be deemed to be in compliance with the provisions of this act.</p>	<p>Dollars (\$50,000.00), or that the affected class of residents to be notified exceeds one hundred thousand (100,000) persons, or that the individual or the entity does not have sufficient contact information or consent to provide notice as described in subparagraph a, b or c of this paragraph.</p>	<p>residents, (2) conspicuous posting of the notice on the Internet web site of the individual or the entity if the individual or the entity maintains a public Internet web site, or (3) notice to major statewide media[.]</p>	<p>individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure;</p> <p>“Encrypted” means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable;</p> <p>“Financial institution” means any institution the business of which is engaging in financial activities as defined by 15 U.S.C. , Section 6809;</p> <p>(a) “Breach of security” means unauthorized acquisition of</p>
Oregon	Oregon Rev. Stat. §	Any person that owns, maintains or otherwise possesses data that	“Personal information”: (a) Means a consumer’s first	The disclosure notification shall be made in the most	Notwithstanding subsection (1) of this section [notification	For purposes of this section, notification to the consumer may be provided by one of the following	Substitute notice consists of the	(a) “Breach of security” means unauthorized acquisition of

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
	646A.600 et seq.	<p>includes a consumer's personal information that is used in the course of the person's business, vocation, occupation or volunteer activities and was subject to a breach of security shall give notice of the breach of security following discovery of such breach of security, or receipt of notification under subsection (2) of this section, to any consumer whose personal information was included in the information that was breached.</p> <p>Any person that maintains or otherwise possesses personal information on behalf of another person shall notify the owner or licensor of the information of any breach of security immediately following discovery of such breach of security if a consumer's personal information was included in the information that was breached.</p>	<p>name or first initial and last name in combination with any one or more of the following data elements, when the data elements are not rendered unusable through encryption, redaction or other methods, or when the data elements are encrypted and the encryption key has also been acquired:</p> <p>(A) Social Security number; (B) Driver license number or state identification card number issued by the Department of Transportation; (C) Passport number or other United States issued identification number; or (D) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account.</p> <p>(b) Means any of the data elements or any combination of the data elements described in paragraph (a) of this subsection when not combined with the consumer's first name or first initial and last name and when the data elements are not rendered unusable through encryption, redaction or other methods, if the information obtained would be sufficient to permit a person to commit identity theft against the consumer whose information was compromised.</p> <p>(c) Does not include</p>	<p>expeditious time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection (3) of this section, and consistent with any measures necessary to determine sufficient contact information for the consumers, determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data.</p> <p>The notification to the consumer required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and that agency has made a written request that the notification be delayed. The notification required by this section shall be made after that law enforcement agency determines that its disclosure will not compromise the investigation and notifies the person in writing.</p>	<p>requirement], notification is not required if, after an appropriate investigation or after consultation with relevant federal, state or local agencies responsible for law enforcement, the person determines that no reasonable likelihood of harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years.</p> <p>This section does not apply to:</p> <p>(a) A person that complies with the notification requirements or breach of security procedures that provide greater protection to personal information and at least as thorough disclosure requirements pursuant to the rules, regulations, procedures, guidance or guidelines established by the person's primary or functional federal regulator. (b) A person that complies with a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breach of security of personal information than that provided by this section. (c) A person that is subject to and complies with regulations promulgated pursuant to Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. 6801 to 6809) as that Act existed on October 1,</p>	<p>methods:</p> <p>(a) Written notice. (b) Electronic notice if the person's customary method of communication with the consumer is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001) as that Act existed on October 1, 2007. (c) Telephone notice, provided that contact is made directly with the affected consumer. (d) Substitute notice, if the person demonstrates that the cost of providing notice would exceed \$250,000, that the affected class of consumers to be notified exceeds 350,000, or if the person does not have sufficient contact information to provide notice.</p> <p>Notice under this section shall include at a minimum:</p> <p>(a) A description of the incident in general terms; (b) The approximate date of the breach of security; (c) The type of personal information obtained as a result of the breach of security; (d) Contact information of the person subject to this section; (e) Contact information for national consumer reporting agencies; and (f) Advice to the consumer to report suspected identity theft to law enforcement, including the Federal Trade Commission.</p> <p>If a person discovers a breach of security affecting more than 1,000 consumers that requires disclosure under this section, the person shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain reports on consumers on a nationwide basis of the timing, distribution and content of the notification given by the person to the consumers. In no case shall a person that is required to make a notification required by this section delay any notification in</p>	<p>following:</p> <p>(A) Conspicuous posting of the notice or a link to the notice on the Internet home page of the person if the person maintains one; and (B) Notification to major statewide television and newspaper media.</p>	<p>computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the person.</p> <p>(b) "Breach of security" does not include good-faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person if the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the personal information.</p> <p>"Encryption" means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
			information, other than a Social Security number, in a federal, state or local government record that is lawfully made available to the public.		2007.	order to make the notification to the consumer reporting agencies. The person shall include the police report number, if available, in its notification to the consumer reporting agencies.		
Pennsylvania	73 Pa. Stat. § 2303	<p>An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person.</p> <p>Encrypted information.--An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.</p> <p>A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making</p>	<p>“Personal information.”</p> <p>(1) An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:</p> <p>(i) Social Security number.</p> <p>(ii) Driver's license number or a State identification card number issued in lieu of a driver's license.</p> <p>(iii) Financial 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.</p> <p>(2) The term does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records.</p>	<p>Except as provided in section 4 [73 P.S. § 2304] or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.</p> <p>The notification required by this act may be delayed if a law enforcement agency determines and advises the entity in writing specifically referencing this section that the notification will impede a criminal or civil investigation. The notification required by this act shall be made after the law enforcement agency determines that it will not compromise the</p>	<p>(a) Information privacy or security policy.--An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and is consistent with the notice requirements of this act shall be deemed to be in compliance with the notification requirements of this act if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.</p> <p>(b) Compliance with Federal requirements.--</p> <p>(1) A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this act.</p> <p>(2) An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures or guidelines established by the entity's primary or functional Federal regulator shall be in compliance with this act.</p>	<p>“Notice.” May be provided by any of the following methods of notification:</p> <p>(1) Written notice to the last known home address for the individual.</p> <p>(2) Telephonic notice, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance.</p> <p>(3) E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual.</p> <p>(4)(i) Substitute notice, if the entity demonstrates one of the following:</p> <p>(A) The cost of providing notice would exceed \$100,000.</p> <p>(B) The affected class of subject persons to be notified exceeds 175,000.</p> <p>(C) The entity does not have sufficient contact information.</p> <p>When an entity provides notification under this act to more than 1,000 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in section 603 of the Fair Credit Reporting Act (Public Law 91-508, 15 U.S.C. § 1681a), of the timing, distribution and number of notices.</p>	<p>Substitute notice shall consist of all of the following:</p> <p>(A) E-mail notice when the entity has an e-mail address for the subject persons.</p> <p>(B) Conspicuous posting of the notice on the entity's Internet website if the entity maintains one.</p> <p>(C) Notification to major Statewide media.</p>	<p>“Breach of the security of the system.” The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth. Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.</p> <p>“Encryption.” The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		the determinations and discharging any remaining duties under this act.		investigation or national or homeland security.				
Rhode Island	R.I. Gen. Laws § 11-49.2-1 et seq.	<p>Any state agency or person that owns, maintains or licenses computerized data that includes personal information, shall disclose any breach of the security of the system which poses a significant risk of identity theft following discovery or notification of the breach in the security of the data to any resident of Rhode Island whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person or a person without authority, to acquire said information.</p> <p>Any state agency or person that maintains computerized unencrypted [sic] data that includes personal information that the state agency or person does not own shall notify the owner or licensee of the information of any breach of the security of the data which poses a significant risk of identity theft immediately, following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>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:</p> <p>(1) Social security number;</p> <p>(2) Driver's license number or Rhode Island Identification Card number;</p> <p>(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.</p>	<p>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.</p> <p>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.</p> <p>The notification must be prompt and reasonable following the determination of the breach unless otherwise provided in this section. Any state agency or person required to make notification under this section and who fails to do so promptly following the determination of a breach or receipt of notice from law</p>	<p>Notification of a breach is not required if, after an appropriate investigation or after consultation with relevant federal, state, or local law enforcement agencies, a determination is made that the breach has not and will not likely result in a significant risk of identity theft to the individuals whose personal information has been acquired.</p> <p>Any state agency or person that maintains its own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of § 11-49.2-3, shall be deemed to be in compliance with the security breach notification requirements of § 11-49.2-3, provided such person notifies subject persons in accordance with such person's policies in the event of a breach of security. Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator, as defined in 15 USC 6809(2), shall be deemed to be in compliance with the security breach notification requirements of this section, provided such person notifies subject persons in accordance with the policies or the rules,</p>	<p>For purposes of this section, "notice" may be provided by one of the following methods:</p> <p>(1) Written notice;</p> <p>(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set for the in Section 7001 of Title 15 of the United States Code;</p> <p>(3) Substitute notice, if the state agency or person demonstrates that the cost of providing notice would exceed twenty-five thousand dollars (\$25,000), or that the affected class of subject persons to be notified exceeds fifty thousand (50,000), or the state agency or person does not have sufficient contact information.</p>	<p>Substitute notice shall consist of all of the following:</p> <p>(A) E-mail notice when the state agency or person has an e-mail address for the subject persons;</p> <p>(B) Conspicuous posting of the notice on the state agency's or person's website page, if the state agency or person maintains one;</p> <p>(C) Notification to major statewide media.</p>	<p>For purposes for this section, "breach of the security of the system" means unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the state agency or person. 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.</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
				enforcement as provided for is subsection (c) is liable for a fine as set forth in § 11-49.2-6.	regulations, procedures or guidelines established by the primary or functional regulator in the event of a breach of security of the system. A financial institution, trust company, credit union or its affiliates that is subject to and examined for, and found in compliance with the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice shall be deemed in compliance with this chapter. A provider of health care, health care service plan, health insurer, or a covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be deemed in compliance with this chapter.			
South Carolina	S.C. Code § 39-1-90	A person conducting business in this State, and owning or licensing computerized data or other data that includes personal identifying information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of this State whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably	“Personal identifying information” has the same meaning as “personal identifying information” in Section 16-13-510(D). § 16-13-510. “Financial identity fraud” and “identifying information” defined; penalty and restitution. (D) “Personal identifying information” means the first name or first initial and last name in combination with and	The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (C), or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	Notwithstanding subsection (E), a person that maintains its own notification procedures as part of an information security policy for the treatment of personal identifying information and is otherwise consistent with the timing requirements of this section is considered to be in compliance with the notification requirements of this section if the person notifies subject persons in accordance with its policies in the event of a breach of security of the system.	The notice required by this section may be provided by: (1) written notice; (2) electronic notice, if the person’s primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures in Section 7001 of Title 15 USC and Chapter 6, Title 11 of the 1976 Code; (3) telephonic notice; or (4) substitute notice, if the person demonstrates that the cost of providing notice exceeds two hundred fifty thousand dollars or that the affected class of subject persons to be notified exceeds five	Substitute notice consists of: (a) e-mail notice when the person has an e-mail address for the subject persons; (b) conspicuous posting of the notice on the web site page of the person, if the person maintains one; or (c) notification to major statewide media.	“Breach of the security of the system” means unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident.</p> <p>A person conducting business in this State and maintaining computerized data or other data that includes personal identifying information that the person does not own shall notify the owner or licensee of the information of a breach of the security of the data immediately following discovery, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>linked to any one or more of the following data elements that relate to a resident of this State, when the data elements are neither encrypted nor redacted:</p> <p>(1) social security number;</p> <p>(2) driver's license number or state identification card number issued instead of a driver's license;</p> <p>(3) financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account;</p> <p>(4) other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual.</p> <p>The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.</p>	<p>The notification required by this section may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. The notification required by this section must be made after the law enforcement agency determines that it no longer compromises the investigation.</p>	<p>This section does not apply to a bank or financial institution that is subject to and in compliance with the privacy and security provision of the Gramm-Leach-Bliley Act.</p> <p>A financial institution that is subject to and in compliance with the federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, as amended, is considered to be in compliance with this section.</p>	<p>hundred thousand or the person has insufficient contact information.</p> <p>If a business provides notice to more than one thousand persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the Department of Consumer Affairs and all consumer reporting agencies that compile and maintain files on a nationwide basis, as defined in 15 USC Section 1681a(p), of the timing, distribution, and content of the notice.</p>	<p>a material risk of harm to a resident. Good faith acquisition of personal identifying information by an employee or agent of the person for the purposes of its business is not a breach of the security of the system if the personal identifying information is not used or subject to further unauthorized disclosure.</p>	
South Dakota	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION	NO PROVISION
Tennessee	Tenn. Code § 47-18-2107, 2010 S.B. 2793	Any information holder 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 Tennessee	Personal information" means an individual's first name or first initial and last name, in combination with any one (1) or more of the following data elements, when either the	The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law	The provisions of this section shall not apply to any person who is subject to the provisions of Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102.	For purposes of this section, notice may be provided by one (1) 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 15 U.S.C. §	Substitute notice shall consist of all of the following: (A) E-mail notice, when the information holder has an e-mail	"Breach of the security of the system" means unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>Any information holder that maintains computerized data that includes personal information that the information holder 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.</p>	<p>name or the data elements are not encrypted:</p> <ul style="list-style-type: none"> (i) Social security number; (ii) Driver license number; or (iii) 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; and <p>(B) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.</p>	<p>enforcement, as provided in subsection (d), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.</p> <p>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.</p>	<p>Notwithstanding subsection (e), an information holder 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 section, 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.</p> <p>When the Tennessee Independent Colleges and Universities Association (TICUA) or any of its member institutions are required by law or by rule or regulation to provide to the Tennessee Higher Education Commission confidential student data or records concerning students enrolled in TICUA institutions, neither TICUA or a member institution shall be held liable in any court of law for any breach of confidentiality of such information, if the breach resulted from actions of the commission or its staff and not from the transmission of the data or records by TICUA or its member institutions before the data or records reached the commission.</p> <p>(b) This section shall apply to any student data or records that are confidential under any law of this state or any federal law, including, but not limited to, the federal Family Educational Rights and Privacy Act, compiled in 20 U.S.C. § 1232g.</p>	<p>7001; or</p> <p>(3) Substitute notice, if the information holder 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 five hundred thousand (500,000), or the information holder does not have sufficient contact information.</p> <p>In the event that a person discovers circumstances requiring notification pursuant to this section of more than one thousand (1,000) persons at one time, the person shall also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a, of the timing, distribution and content of the notices.</p>	<p>address for the subject persons;</p> <p>(B) Conspicuous posting of the notice on the information holder's internet website page, if the information holder maintains such website page; and</p> <p>(C) Notification to major statewide media.</p>	<p>integrity of personal information maintained by the information holder. Good faith acquisition of personal information by an employee or agent of the information holder for the purposes of the information holder is not a breach of the security of the system; provided, that the personal information is not used or subject to further unauthorized disclosure;</p> <p>"Information holder" means any person or business that conducts business in this state, or any agency of the state of Tennessee or any of its political subdivisions, that owns or licenses computerized data that includes personal information;</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
Texas	Tex. Bus. & Com. Code §§ 521.002, 521.03	<p>Text of subsection effective until September 01, 2012: (b) A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any resident of this state whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>Text of subsection effective on September 01, 2012 A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>Text of subsection effective on September 01, 2012 (b-1) Notwithstanding Subsection (b), the requirements of Subsection (b) apply only if the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident of this state or another state that</p>	<p>Personal identifying information" means information that alone or in conjunction with other information identifies an individual, including an individual's:(A) name, social security number, date of birth, or government-issued identification number;(B) mother's maiden name;(C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;(D) unique electronic identification number, address, or routing code; and(E) telecommunication access device as defined by Section 32.51, Penal Code.</p> <p>"Sensitive personal information" means, subject to Subsection (b):(A) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:(i) social security number;(ii) driver's license number or government-issued identification number; or(iii) account number or 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; or(B)</p>	<p>The disclosure shall be made as quickly as possible, except as provided by Subsection (d) [law enforcement delay] or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.</p> <p>(d) A person may delay providing notice as required by Subsection (b) or (c) at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation.</p>	<p>(g) Notwithstanding Subsection (e), a person who maintains the person's own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person notifies affected persons in accordance with that policy.</p>	<p>(e) A person may give notice as required by Subsection (b) or (c) by providing:(1) written notice;(2) electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001; or(3) notice as provided by Subsection (f) [substitute notice].</p> <p>(h) If a person is required by this section to notify at one time more than 10,000 persons of a breach of system security, the person shall also notify each consumer reporting agency, as defined by 15 U.S.C. Section 1681a, that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices. The person shall provide the notice required by this subsection without unreasonable delay.</p>	<p>(f) If the person required to give notice under Subsection (b) or (c) demonstrates that the cost of providing notice would exceed \$250,000, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information, the notice may be given by:(1) electronic mail, if the person has electronic mail addresses for the affected persons;(2) conspicuous posting of the notice on the person's website; or(3) notice published in or broadcast on major statewide media.</p>	<p>"breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner.</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>does not require a person described by Subsection (b) to notify the individual of a breach of system security. If the individual is a resident of a state that requires a person described by Subsection (b) to provide notice of a breach of system security, the notice of the breach of system security provided under that state's law satisfies the requirements of Subsection (b).</p> <p>(c) Any person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>information that identifies an individual and relates to:(i) the physical or mental health or condition of the individual;(ii) the provision of health care to the individual; or(iii) payment for the provision of health care to the individual.(b) For purposes of this chapter, the term "sensitive personal information" does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.</p>					
Utah	Utah Code Title 13, Chapter 44	<p>(a) A person who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the person becomes aware of a breach of system security, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes.</p> <p>(b) If an investigation under Subsection (1)(a) reveals that the misuse of personal information for identity theft or fraud</p>	<p>"Personal information" means a person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or date element is unencrypted or not protected by another method that renders the data unreadable or unusable: (i) Social Security number; (ii)(A) financial account number, or credit or debit card number; and (B) any required security code, access code, or password that</p>	<p>A person required to provide notification under Subsection (1) shall provide the notification in the most expedient time possible without unreasonable delay: (a) considering legitimate investigative needs of law enforcement, as provided in Subsection (4)(a); (b) after determining the scope of the breach of system security; and (c) after restoring the reasonable integrity of the system.</p>	<p>If a person maintains the person's own notification procedures as part of an information security policy for the treatment of personal information the person is considered to be in compliance with this chapter's notification requirements if the procedures are otherwise consistent with this chapter's timing requirements and the person notifies each affected Utah resident in accordance with the person's information security policy in the event of a breach.</p> <p>A person who is regulated by state or federal law and maintains</p>	<p>A notification required by this section may be provided: (i) in writing by first-class mail to the most recent address the person has for the resident; (ii) electronically, if the person's primary method of communication with the resident is by electronic means, or if provided in accordance with the consumer disclosure provisions of 15 U.S.C. Section 7001; (iii) by telephone, including through the use of automatic dialing technology not prohibited by other law; or (iv) by publishing notice of the breach of system security: (A) in a newspaper of general circulation ; and (B) as required in Section 45-1-101.</p>	<p>§ 45-1-101. Legal notice publication requirements*** (2) Except as provided in Subsections (8) and (9), notwithstanding any other legal notice provision established by law, a person required by law to publish legal notice shall publish the notice: (a) as required by the statute establishing the legal notice requirement; and</p>	<p>(a) "Breach of system security" means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information. (b) "Breach of system security" does not include the acquisition of personal information by an employee or agent of the person possessing unencrypted computerized data unless the personal information is used for an unlawful purpose or disclosed in an unauthorized</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>purposes has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident.</p> <p>A person who maintains computerized data that includes personal information that the person does not own or license shall notify and cooperate with the owner or licensee of the information of any breach of system security immediately following the person's discovery of the breach if misuse of the personal information occurs or is reasonably likely to occur. Cooperation under Subsection (3)(a) includes sharing information relevant to the breach with the owner or licensee of the information.</p>	<p>would permit access to the person's account; or (iii) driver license number or state identification card number.</p> <p>"Personal information" does not include information regardless of its source, contained in federal, state, or local government records or in widely distributed media that are lawfully made available to the general public.</p>	<p>Notwithstanding Subsection (2), a person may delay providing notification under Subsection (1) at the request of a law enforcement agency that determines that notification may impede a criminal investigation.</p> <p>A person who delays providing notification under Subsection (4)(a) shall provide notification in good faith without unreasonable delay in the most expedient time possible after the law enforcement agency informs the person that notification will no longer impede the criminal investigation.</p>	<p>procedures for a breach of system security under applicable law established by the primary state or federal regulator is considered to be in compliance with this part if the person notifies each affected Utah resident in accordance with the other applicable law in the event of a breach.</p>		<p>(b) on a public legal notice website established by the combined efforts of Utah's newspapers that collectively distribute newspapers to the majority of newspaper subscribers in the state. ***</p>	<p>manner.</p>
Vermont	Vt. Stat. tit. 9 § 2430 et seq.	<p>Except as set forth in subsection (d) of this section, any data collector that owns or licenses computerized personal information that includes personal information concerning a consumer shall notify the consumer that there has been a security breach following discovery or notification to the data collector of the breach.</p> <p>Any data collector that maintains or possesses computerized data containing personal information of a consumer that the business does not own or license or any data collector that conducts business in Vermont that maintains or possesses records</p>	<p>"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 or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons:</p> <p>(i) Social Security number;</p> <p>(ii) Motor vehicle operator's license number or nondriver identification card number;</p> <p>(iii) Financial account number or credit or debit card number, if circumstances exist in which the number could be used</p>	<p>Notice of the breach shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of the law enforcement agency, as provided in subdivision (3) of this subsection, or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.</p> <p>The notice required by this subsection shall be delayed upon request of a law enforcement agency. A law</p>	<p>Notice of a security breach pursuant to subsection (b) of this section is not required if the data collector establishes that misuse of personal information is not reasonably possible and the data collector provides notice of the determination that the misuse of the personal information is not reasonably possible pursuant to the requirements of this subsection. If the data collector establishes that misuse of the personal information is not reasonably possible, the data collector shall provide notice of its determination that misuse of the personal information is not reasonably possible and a detailed explanation for said determination</p>	<p>The notice shall be clear and conspicuous. The notice shall include a description of the following:</p> <p>(A) The incident in general terms.</p> <p>(B) The type of personal information that was subject to the unauthorized access or acquisition.</p> <p>(C) The general acts of the business to protect the personal information from further unauthorized access or acquisition.</p> <p>(D) A toll-free telephone number that the consumer may call for further information and assistance.</p> <p>(E) Advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports.</p> <p>(5) For purposes of this subsection, notice to consumers may be provided by one of the following methods:</p> <p>(A) Direct notice to consumers, which may be by one of the following methods:</p> <p>(i) Written notice mailed to the consumer's residence;</p>	<p>Substitute notice shall consist of all of the following:</p> <p>(i) conspicuous posting of the notice on the data collector's website page if the data collector maintains one; and</p> <p>(ii) notification to major statewide and regional media.</p>	<p>"Data collector" may include, but is not limited to, the state, state agencies, political subdivisions of the state, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, retail operators, and any other entity that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information.</p> <p>"Encryption" means use of an algorithmic process to transform data into a form in</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>or data containing personal information that the data collector does not own or licensee shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subdivision (3) of this subsection.</p> <p>If a data collector established that misuse of personal information was not reasonably possible under subdivision (1) of this subsection, and subsequently obtains facts indicating that misuse of the personal information has occurred or is occurring, the data collector shall provide notice of the security breach pursuant to subsection (b) of this section.</p>	<p>without additional identifying information, access codes, or passwords;</p> <p>(iv) Account passwords or personal identification numbers or other access codes for a financial account.</p> <p>(B) "Personal information" does not mean publicly available information that is lawfully made available to the general public from federal, state, or local government records.</p>	<p>enforcement agency may request the delay if it believes that notification may impede a law enforcement investigation, or a national or homeland security investigation or jeopardize public safety or national or homeland security interests. In the event law enforcement makes the request in a manner other than in writing, the data collector shall document such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. A law enforcement agency shall promptly notify the data collector when the law enforcement agency no longer believes that notification may impede a law enforcement investigation, or a national or homeland security investigation or jeopardize public safety or national or homeland security interests. The data collector shall provide notice required by this section without unreasonable delay upon receipt of a written communication, which includes facsimile or</p>	<p>to the Vermont attorney general or to the department of banking, insurance, securities, and health care administration in the event that the data collector is a person or entity licensed or registered with the department under Title 8 or this title. The data collector may designate its notice and detailed explanation to the Vermont attorney general or the department of banking, insurance, securities, and health care administration as "trade secret" if the notice and detailed explanation meet the definition of trade secret contained in subdivision 317(c)(9) of Title 1.</p> <p>A financial institution that is subject to the following guidances, and any revisions, additions, or substitutions relating to said interagency guidance shall be exempt from this section:</p> <p>(1) The Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision; or</p> <p>(2) Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration.</p>	<p>(ii) Electronic notice, for those consumers for whom the data collector has a valid e-mail address if:</p> <p>(I) the data collector does not have contact information set forth in subdivisions (i) and (iii) of this subdivision (5)(A), the data collector's primary method of communication with the consumer is by electronic means, the electronic notice does not request or contain a hypertext link to a request that the consumer provide personal information, and the electronic notice conspicuously warns consumers not to provide personal information in response to electronic communications regarding security breaches; or</p> <p>(II) the notice provided is consistent with the provisions regarding electronic records and signatures for notices as set forth in 15 U.S.C. § 7001; or</p> <p>(iii) Telephonic notice, provided that telephonic contact is made directly with each affected consumer, and the telephonic contact is not through a prerecorded message.</p> <p>(B) Substitute notice, if the data collector demonstrates that the cost of providing written or telephonic notice, pursuant to subdivision (A)(i) or (iii) of this subdivision (5), to affected consumers would exceed \$5,000.00 or that the affected class of affected consumers to be provided written or telephonic notice, pursuant to subdivision (A)(i) or (iii) of this subdivision (5), exceeds 5,000, or the data collector does not have sufficient contact information.</p> <p>In the event a data collector provides notice to more than 1,000 consumers at one time pursuant to this section, the data collector shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice. This subsection shall not apply to a person who is licensed or registered under Title 8 by the department of banking,</p>	<p>which the data is rendered unreadable or unusable without use of a confidential process or key.</p> <p>"Security breach" means unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector.</p> <p>(B) "Security breach" does not include good faith but unauthorized acquisition or access of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.</p>	<p>which the data is rendered unreadable or unusable without use of a confidential process or key.</p> <p>"Security breach" means unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector.</p> <p>(B) "Security breach" does not include good faith but unauthorized acquisition or access of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
				electronic communication, from the law enforcement agency withdrawing its request for delay.		insurance, securities, and health care administration.		
Virginia	Va. Code § 18.2-186.6 [personal information], § 32.1-127.1:05 [medical information]	If unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, an individual or entity 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 of the security of the system to the Office of the Attorney General and any affected resident of the Commonwealth without unreasonable delay. An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth. An individual or entity that	"Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted: 1. Social security number; 2. Driver's license number or state identification card number issued in lieu of a driver's license number; or 3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts. The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public. <i>Medical Information:</i> "Medical information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements	"without unreasonable delay" Notice required by this section may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system. Notice required by this section may be delayed if, after the individual or entity notifies a law-enforcement agency, the law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security. <i>Medical Information:</i> "without unreasonable delay" Notice required by this	An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information that are consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if it notifies residents of the Commonwealth in accordance with its procedures in the event of a breach of the security of the system. An entity that is subject to Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) and maintains procedures for notification of a breach of the security of the system in accordance with the provision of that Act and any rules, regulations, or guidelines promulgated thereto shall be deemed to be in compliance with this section. An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional state or federal regulator shall be in compliance with this section. The provisions of this section shall not apply to criminal intelligence	"Notice" means: 1. Written notice to the last known postal address in the records of the individual or entity; 2. Telephone notice; 3. Electronic notice; or 4. Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed \$50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or consent to provide notice as described in subdivisions 1, 2, or 3 of this definition. Notice required by this section shall not be considered a debt communication as defined by the Fair Debt Collection Practices Act in 15 U.S.C. § 1692a. Notice required by this section shall include a description of the following: (1) The incident in general terms; (2) The type of personal information that was subject to the unauthorized access and acquisition; (3) The general acts of the individual or entity to protect the personal information from further unauthorized access; (4) A telephone number that the person may call for further information and assistance, if one exists; and (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. In the event an individual or entity provides notice to more than 1,000 persons at one time pursuant to this section, the individual or entity shall notify, without unreasonable delay, the Office of the Attorney General and all consumer reporting agencies that compile and maintain files on	Substitute notice consists of all of the following: a. E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents; b. Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and c. Notice to major statewide media. <i>Medical Information:</i> Substitute notice consists of the following: a. E-mail notice if the entity has e-mail addresses for the members of the affected class of residents; b. Conspicuous posting of the notice on the website of the entity if the entity maintains a website; and c. Notice to major statewide media.	"Breach of the security of the system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure. "Encrypted" means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system, if the personal information was accessed and acquired by an unauthorized person or the individual or entity reasonably believes the personal information was accessed and acquired by an unauthorized person.</p> <p><i>Medical Information:</i></p> <p>If unencrypted or unredacted medical information was or is reasonably believed to have been accessed and acquired by an unauthorized person, an entity that owns or licenses computerized data that includes medical information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to the Office of the Attorney General, the Commissioner of Health, the subject of the medical information, and any affected resident of the Commonwealth without unreasonable delay. An entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an</p>	<p>that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:</p> <p>1. Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or</p> <p>2. An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.</p> <p>The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.</p>	<p>section may be reasonably delayed to allow the entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system. Notice required by this section may be delayed if, after the entity notifies a law-enforcement agency, the law-enforcement agency determines and advises the entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.</p>	<p>systems subject to the restrictions of 28 C.F.R. Part 23 that are maintained by law-enforcement agencies of the Commonwealth and the organized Criminal Gang File of the Virginia Criminal Information Network (VCIN), established pursuant to Chapter 2 (§ 52-12 et seq.) of Title 52.</p> <p><i>Medical Information:</i></p> <p>This section shall not apply to (i) a person or entity who is a "covered entity" or "business associate" under the Health Insurance Portability and Accountability Act of 1996 (42 USC § 1320d et seq.) and is subject to requirements for notification in the case of a breach of protected health information (42 USC 17932 et seq.) or (ii) a person or entity who is a non-HIPAA-covered entity subject to the Health Breach Notification Rule promulgated by the Federal Trade Commission pursuant to 42 USC § 17937 et seq.</p> <p>G. An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, and guidelines established by the entity's primary or functional state or federal regulator shall be in compliance with this section.</p>	<p>consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice.</p> <p><i>Medical Information:</i></p> <p>"Notice" means:</p> <ol style="list-style-type: none"> 1. Written notice to the last known postal address in the records of the entity; 2. Telephone notice; 3. Electronic notice; or 4. Substitute notice, if the entity required to provide notice demonstrates that the cost of providing notice will exceed \$50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the entity does not have sufficient contact information or consent to provide notice as described in subdivisions 1, 2, or 3 of this definition. <p>Notice required by this section shall include a description of the following:</p> <ol style="list-style-type: none"> (1) The incident in general terms; (2) The type of medical information that was subject to the unauthorized access and acquisition; (3) The general acts of the entity to protect the personal information from further unauthorized access; and (4) A telephone number that the person may call for further information and assistance, if one exists. <p>In the event an entity provides notice to more than 1,000 persons at one time, pursuant to this section, the entity shall notify, without unreasonable delay, the Office of the Attorney General and the Commissioner of Health of the timing, distribution, and content of the notice.</p>	<p>use of a confidential process or key, or the securing of the information by another method that renders the data elements unreadable or unusable.</p> <p>"Financial institution" has the meaning given that term in 15 U.S.C. § 6809(3).</p> <p><i>Medical Information:</i></p> <p>"Breach of the security of the system" means unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of medical information maintained by an entity. Good faith acquisition of medical information by an employee or agent of an entity for the purposes of the entity is not a breach of the security of the system, provided that the medical information is not used for a purpose other than a lawful purpose of the entity or subject to further unauthorized disclosure.</p>	

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>unencrypted form, or if the security breach involves a person with access to the encryption key.</p> <p>An entity that maintains computerized data that includes medical information that the entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system, if the medical information was accessed and acquired by an unauthorized person or the entity reasonably believes the medical information was accessed and acquired by an unauthorized person.</p>						

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
Washington	Wash. Rev. Code § 19.255.010, 42.56.590 [state agencies]	<p>Any person or business that conducts business in this state 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 this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>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.</p>	<p>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:</p> <p>(a) Social security number;</p> <p>(b) Driver's license number or Washington identification card number; or</p> <p>(c) Account number or 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.</p> <p>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.</p>	<p>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 subsection (3) of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.</p> <p>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.</p>	<p>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 section is 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.</p> <p>A person or business under this section shall not be required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of criminal activity.</p>	<p>For purposes of this section and except under subsection (8) of this section, "notice" may be provided by one of the following methods:</p> <p>(a) Written notice;</p> <p>(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001; or</p> <p>(c) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person or business does not have sufficient contact information.</p>	<p>Substitute notice shall consist of all of the following:</p> <p>(i) E-mail notice when the person or business has an e-mail address for the subject persons;</p> <p>(ii) Conspicuous posting of the notice on the web site page of the person or business, if the person or business maintains one; and</p> <p>(iii) Notification to major statewide media.</p>	<p>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 when the personal information is not used or subject to further unauthorized disclosure.</p>
West Virginia	W.V. Code §§ 46A-2A-101 et seq.	<p>An individual or entity that owns or licenses computerized data that includes personal information shall give notice of any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of this state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity</p>	<p>Personal information" means the first name or first initial and last name linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor redacted:</p> <p>(A) Social security number;</p> <p>(B) Driver's license number or state identification card number issued in lieu of a driver's license; or</p> <p>(C) Financial account number, or credit card, or debit card</p>	<p>Except as provided in subsection (e) of this section or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the notice shall be made without unreasonable delay.</p>	<p>Notice required by this section may be delayed if a law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation or homeland or national security. Notice required by this section must be made without unreasonable delay after the law-enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security.</p>	<p>Notice" means:</p> <p>(A) Written notice to the postal address in the records of the individual or entity;</p> <p>(B) Telephonic notice;</p> <p>(C) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures, set forth in Section 7001, United States Code Title 15, Electronic Signatures in Global and National Commerce Act.</p> <p>(D) Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed fifty thousand dollars or that the affected class of residents to be notified exceeds one hundred thousand persons or that the individual or the entity does not have</p>	<p>Substitute notice consists of any two of the following:</p> <p>(i) E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents;</p> <p>(ii) Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a</p>	<p>"Breach of the security of a system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the breach of security has caused</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state.</p> <p>An individual or entity must give notice of the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of this state.</p> <p>(c) An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery, if the personal information was or the entity reasonably believes was accessed and acquired by an unauthorized person.</p>	<p>number in combination with any required security code, access code or password that would permit access to a resident's financial accounts.</p> <p>The term does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.</p>		<p>An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of this article shall be deemed to be in compliance with the notification requirements of this article if it notifies residents of this state in accordance with its procedures in the event of a breach of security of the system.</p> <p>A financial institution that responds in accordance with the notification guidelines prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this article.</p> <p>An entity that complies with the notification requirements or procedures pursuant to the rules, regulation, procedures or guidelines established by the entity's primary or functional regulator shall be in compliance with this article.</p>	<p>sufficient contact information or to provide notice as described in paragraph (A), (B) or (C).</p> <p>The notice shall include: (1) To the extent possible, a description of the categories of information that were reasonably believed to have been accessed or acquired by an unauthorized person, including social security numbers, driver's licenses or state identification numbers and financial data; (2) A telephone number or website address that the individual may use to contact the entity or the agent of the entity and from whom the individual may learn: (A) What types of information the entity maintained about that individual or about individuals in general; and (B) Whether or not the entity maintained information about that individual. (3) The toll-free contact telephone numbers and addresses for the major credit reporting agencies and information on how to place a fraud alert or security freeze.</p> <p>If an entity is required to notify more than one thousand persons of a breach of security pursuant to this article, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on a nationwide basis, as defined by 15 U.S.C. §1681a (p), of the timing, distribution and content of the notices. Nothing in this subsection shall be construed to require the entity to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients. This subsection shall not apply to an entity who is subject to Title V of the Gramm Leach Bliley Act, 15 U.S.C. 6801, et seq.</p> <p>The notice required by this section shall not be considered a debt communication as defined by the</p>	<p>website; or (iii) Notice to major statewide media.</p>	<p>or will cause identity theft or other fraud to any resident of this state. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.</p> <p>"Encrypted" means transformation of data through the use of an algorithmic process to into a form in which there is a low probability of assigning meaning without use of a confidential process or key or securing the information by another method that renders the data elements unreadable or unusable.</p> <p>"Financial institution" has the meaning given that term in Section 6809(3), United States Code Title 15, as amended.</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
Wisconsin	Wis. Stat. § 134.98 et seq.	<p>If an entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each subject of the personal information.</p> <p>If an entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each resident of this state who is the subject of the personal information.</p> <p>If a person, other than an individual, that stores personal information pertaining to a resident of this state, but does not own or license the personal information, knows that the personal information has been acquired by a person whom the person storing the personal information has not authorized to acquire the personal information, and the person storing the personal information has not</p>	<p>"Personal information" means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable:</p> <ol style="list-style-type: none"> 1. The individual's social security number. 2. The individual's driver's license number or state identification number. 3. The number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account. 4. The individual's deoxyribonucleic acid profile, as defined in s. 939.74(2d)(a). 5. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation. 	<p>Subject to sub. (5), an entity shall provide the notice required under sub. (2) within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information. A determination as to reasonableness under this paragraph shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity.</p> <p>A law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to provide a notice that is otherwise required under sub. (2) for any period of time and the notification process required under sub. (2) shall begin at the end of that time period.</p> <p>Notwithstanding subs. (2) and (3), if an entity receives such a request, the entity may not provide notice of or publicize an unauthorized acquisition of personal information, except as authorized by the law enforcement agency that made the request.</p>	<p>[A]n entity is not required to provide notice of the acquisition of personal information if any of the following applies:</p> <ol style="list-style-type: none"> 1. The acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information. 2. The personal information was acquired in good faith by an employee or agent of the entity, if the personal information is used for a lawful purpose of the entity. <p>This section does not apply to any of the following:</p> <ol style="list-style-type: none"> (a) An entity that is subject to, and in compliance with, the privacy and security requirements of 15 USC 6801 to 6827, or a person that has a contractual obligation to such an entity, if the entity or person has in effect a policy concerning breaches of information security. (b) An entity that is described in 45 CFR 164.104(a), if the entity complies with the requirements of 45 CFR part 164. 	<p>Fair Debt Collection Practice Act in 15 U.S.C. §1692a.</p> <p>The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information.</p> <p>If, as the result of a single incident, an entity is required under par. (a) or (b) to notify 1,000 or more individuals that personal information pertaining to the individuals has been acquired, the entity shall without unreasonable delay notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the timing, distribution, and content of the notices sent to the individuals.</p> <p>An entity shall provide the notice required under sub. (2) by mail or by a method the entity has previously employed to communicate with the subject of the personal information. [If an entity cannot with reasonable diligence determine the mailing address of the subject of the personal information, and if the entity has not previously communicated with the subject of the personal information, the entity shall provide notice by a method reasonably calculated to provide actual notice to the subject of the personal information.]</p> <p>Upon written request by a person who has received a notice under sub. (2)(a) or (b), the entity that provided the notice shall identify the personal information that was acquired.</p>	<p>[If an entity cannot with reasonable diligence determine the mailing address of the subject of the personal information, and if the entity has not previously communicated with the subject of the personal information, the entity shall provide notice by a method reasonably calculated to provide actual notice to the subject of the personal information.]</p>	<p>"Entity" means a person, other than an individual, that does any of the following:</p> <ol style="list-style-type: none"> a. Conducts business in this state and maintains personal information in the ordinary course of business. b. Licenses personal information in this state. c. Maintains for a resident of this state a depository account as defined in s. 815.18(2)(e). d. Lends money to a resident of this state. <p>"Entity" includes all of the following:</p> <ol style="list-style-type: none"> a. The state and any office, department, independent agency, authority, institution, association, society, or other body in state government created or authorized to be created by the constitution or any law, including the legislature and the courts. b. A city, village, town, or county. <p>"Name" means an individual's last name combined with the individual's first name or first initial.</p> <p>"Publicly available information" means any information that an entity reasonably believes is one of the following:</p> <ol style="list-style-type: none"> 1. Lawfully made widely available through any media.

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		entered into a contract with the person that owns or licenses the personal information, the person storing the personal information shall notify the person that owns or licenses the personal information of the acquisition as soon as practicable.						2. Lawfully made available to the general public from federal, state, or local government records or disclosures to the general public that are required to be made by federal, state, or local law.
Wyoming	Wyo. Stat. § 40-12-501 to - 502	An individual or commercial entity that conducts business in Wyoming and that owns or licenses computerized data that includes personal identifying information about a resident of Wyoming shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal identifying information has been or will be misused. If the investigation determines that the misuse of personal identifying information about a Wyoming resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected Wyoming resident. Any person who maintains computerized data that includes personal identifying information on behalf of another business entity shall disclose to the business entity for which the information is maintained any breach of the security of the system as soon as practicable following the determination that	“Personal identifying information” means the first name or first initial and last name of a person in combination with one (1) or more of the following data elements when either the name or the data elements are not redacted: (A) Social security number; (B) Driver’s license number or Wyoming identification card number; (C) Account number, credit card number or debit card number in combination with any security code, access code or password that would allow access to a financial account of the person; (D) Tribal identification card; or (E) Federal or state government issued identification card. “Personal identifying information” as defined in paragraph (a)(vii) of this section does not include information, regardless of its source, contained in any federal, state or local government records or in widely distributed media that are lawfully made available to	Notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. The notification required by this section may be delayed if a law enforcement agency determines in writing that the notification may seriously impede a criminal investigation.	Any financial institution as defined in 15 U.S.C. 6809 or federal credit union as defined by 12 U.S.C. 1752 that maintains notification procedures subject to the requirements of 15 U.S.C. 6801(b)(3) and 12 C.F.R. Part 364 Appendix B or Part 748 Appendix B, is deemed to be in compliance with this section if the financial institution notifies affected Wyoming customers in compliance with the requirements of 15 U.S.C. 6801 through 6809 and 12 C.F.R. Part 364 Appendix B or Part 748 Appendix B.	For purposes of this section, notice to consumers may be provided by one (1) of the following methods: (i) Written notice; (ii) Electronic mail notice; (iii) Substitute notice, if the person demonstrates: (A) That the cost of providing notice would exceed ten thousand dollars (\$10,000.00) for Wyoming-based persons or businesses, and two hundred fifty thousand dollars (\$250,000.00) for all other businesses operating but not based in Wyoming; (B) That the affected class of subject persons to be notified exceeds ten thousand (10,000) for Wyoming-based persons or businesses and five hundred thousand (500,000) for all other businesses operating but not based in Wyoming; or (C) The person does not have sufficient contact information. Notice required under subsection (a) of this section shall include: (i) A toll-free number: (A) That the individual may use to contact the person collecting the data, or his agent; and (B) From which the individual may learn the toll-free contact telephone numbers and addresses for the major credit reporting agencies.	Substitute notice” means: (A) An electronic mail notice when the person or business has an electronic mail address for the subject persons; (B) Conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; and (C) Publication in applicable local or statewide media. Substitute notice shall consist of all of the following: (A) Conspicuous posting of the notice on the Internet, the World Wide Web or a similar proprietary or common carrier electronic system site of the person collecting the data, if the person maintains a public Internet, the World Wide Web or a	“Breach of the security of the data system” means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal identifying information maintained by a person or business and causes or is reasonably believed to cause loss or injury to a resident of this state. Good faith acquisition of personal identifying information by an employee or agent of a person or business for the purposes of the person or business is not a breach of the security of the data system, provided that the personal identifying information is not used or subject to further unauthorized disclosure; Financial institution” means any person licensed or chartered under the laws of any state or the United States as a bank holding company, bank, savings and loan association, credit union, trust company or subsidiary thereof doing business in this state;

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person. The person who maintains the data on behalf of another business entity and the business entity on whose behalf the data is maintained may agree which person or entity will provide any required notice as provided in subsection (a) of this section, provided only a single notice for each breach of the security of the system shall be required. If agreement regarding notification cannot be reached, the person who has the direct business relationship with the resident of this state shall provide notice subject to the provisions of subsection (a) of this section.	the general public				similar proprietary or common carrier electronic system site; and (B) Notification to major statewide media. The notice to media shall include a toll-free phone number where an individual can learn whether or not that individual's personal data is included in the security breach.	
District of Columbia	D.C. Code § 28- 3851 et seq.	Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information, and who discovers a breach of the security of the system, shall promptly notify any District of Columbia resident whose personal information was included in the breach. Any person or entity who maintains, handles, or otherwise possesses computerized or other electronic data that includes personal information that the person or entity does not own	“Personal information” means: (i) An individual's first name or first initial and last name, or phone number, or address, and any one or more of the following data elements: (I) Social security number; (II) Driver's license number or District of Columbia Identification Card number; or (III) Credit card number or debit card number; or (ii) Any other number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account.	The notification shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (d) of this section, and with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a	Notwithstanding subsection (a) of this section, 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 subchapter shall be deemed to be in compliance with the notification requirements of this section if the person or business provides notice, in accordance with its policies, reasonably calculated to give actual notice to persons to whom notice is otherwise required to be given under this subchapter. Notice under this section may be given by electronic mail if the person or entity's primary method	“Notify” or “notification” means providing information through any of the following methods: (A) Written notice; (B) Electronic notice, if the customer has consented to receipt of electronic notice consistent with the provisions regarding electronic records and signatures set forth in the Electronic Signatures in Global and National Commerce Act, approved June 30, 2000 (114 Stat. 641; 15 U.S.C.S. § 7001); or (C)(i) Substitute notice, if the person or business demonstrates that the cost of providing notice to persons subject to this subchapter would exceed \$50,000, that the number of persons to receive notice under this subchapter exceeds 100,000, or that the person or business does not have sufficient contact information. If any person or entity is required by subsection (a) or (b) of this section to notify more than 1,000 persons of a breach of security pursuant to this	Substitute notice shall consist of all of the following: (I) E-mail notice when the person or business has an e-mail address for the subject persons; (II) Conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; and (III) Notice to major local and, if applicable, national media.	“Breach of the security of the system” means unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data, that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. The term “breach of the security system” shall not include a good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business if the personal information is not used improperly or subject to further unauthorized

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		shall notify the owner or licensee of the information of any breach of the security of the system in the most expedient time possible following discovery.	For purposes of this paragraph, the term "personal information" shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.	criminal investigation but shall be made as soon as possible after the law enforcement agency determines that the notification will not compromise the investigation.	of communication with the resident is by electronic means. A person or entity who maintains procedures for a breach notification system under Title V of the Gramm-Leach-Bliley Act, approved November 12, 1999 (113 Stat. 1436; 15 U.S.C § 6801 et seq.) ("Act"), and provides notice in accordance with the Act, and any rules, regulations, guidance and guidelines thereto, to each affected resident in the event of a breach, shall be deemed to be in compliance with this section.	subsection, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by section 603(p) of the Fair Credit Reporting Act, approved October 26, 1970 (84 Stat. 1128; 15 U.S.C. § 1681a(p)), of the timing, distribution and content of the notices. Nothing in this subsection shall be construed to require the person to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients. This subsection shall not apply to a person or entity who is required to notify consumer reporting agencies of a breach pursuant to Title V of the Gramm-Leach-Bliley Act, approved November 12, 1999 (113 Stat. 1436; 15 U.S.C § 6801 et seq).		disclosure. Acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party, shall not be deemed to be a breach of the security of the system.
Guam	9 Guam Code Chapter 48	An individual or entity 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 of the security of the system to any resident of Guam whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of Guam. An individual or entity must disclose the breach of the security of the system if encrypted information is accessed and acquired in	Personal information means the first name, or first initial, and last name in combination with and linked to any one or more of the following data elements that relate to a resident of Guam, when the data elements are neither encrypted nor redacted: (1) Social Security number; (2)Driver's license number or Guam identification card number issued in lieu of a driver's license; or (3) Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts. (4) The term does not include information that is lawfully obtained from publicly available information, or from	Except as provided in subsection (d) of this Section, or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the disclosure shall be made without unreasonable delay. Notice required by this Section may be delayed if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice required by this Section must be made without unreasonable delay after the law enforcement agency determines that notification will no longer	An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of this Chapter shall be deemed to be in compliance with the notification requirements of this Chapter if it notifies residents of Guam in accordance with its procedures in the event of a breach of security of the system. (b) Compliance with Federal requirements. (1) A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this Chapter. (2) An entity that complies with the	Notice means: (1) Written notice to the postal address in the records of the individual or entity; (2) Telephone notice; (3) Electronic notice; or (4) Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed Ten Thousand Dollars (\$10,000), or that the affected class of residents to be notified exceeds five thousand (5,000) persons, or that the individual or the entity does not have sufficient contact information or consent to provide notice as described in Paragraphs 1, 2, or 3.	Substitute notice consists of any two (2) of the following: (A) E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents; (B) Conspicuous posting of the notice on the Website of the individual or the entity, if the individual or the commercial entity maintains a Website; and (C) Notice to major Guam media.	Breach of the security of a system means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of Guam. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided, that the personal

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		<p>unencrypted form, or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of Guam.</p> <p>An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery, if the personal information was, or if the entity reasonably believes was, accessed and acquired by an unauthorized person.</p>	Federal, State, or local government records lawfully made available to the general public.	impede the investigation or jeopardize national or homeland security.	notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional Federal regulator shall be in compliance with this Chapter.			<p>information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.</p> <p>Encrypted means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable.</p> <p>Financial institution has the meaning given that term in Section 6809(3) of Title 15, United States Code.</p>
Puerto Rico	<p>10 Laws of Puerto Rico § 4051 et. seq.</p> <p><i>[The laws of PR are published for convenience in both English and Spanish, but the Spanish version is authoritative. Please check the Spanish version for statutory text.]</i></p>	<p>Any entity that is the owner or custodian of a database that includes personal information of citizens residents of Puerto Rico must notify said citizens of any breach of the security of the system when the database whose security has been breached contains, in whole or in part, personal information files and the same are not protected by an encrypted code but only by a password.</p> <p>Any entity that as part of their operations resells or provides access to digital data banks that at the same time contain personal information files of citizens must notify the proprietor, custodian or holder of</p>	<p>Personal information file.-- Refers to a file containing at least the name or first initial and the surname of a person, together with any of the following data so that an association may be established between certain information with another and in which the information is legible enough so that in order to access it there is no need to use a special cryptographic code.</p> <p>(1) Social security number. (2) Driver's license number, voter's identification or other official identification. (3) Bank or financial account numbers of any type with or without passwords or access</p>	<p>Clients must be notified as expeditiously as possible, taking into consideration the need of law enforcement agencies to secure possible crime scenes and evidence as well as the application of measures needed to restore the system's security.</p> <p>Within a non-extendable term of ten (10) days after the violation of the system's security has been detected, the parties responsible shall inform the Department, which shall make a public announcement of the fact within twenty-four (24) hours after having received the information.</p>	<p>No provision of this chapter shall be interpreted as being prejudicial to those institutional information and security policies that an enterprise or entity may have in force prior to its effectiveness and whose purpose is to provide protection equal or better to the information on security herein established.</p> <p>In those cases in which the breach or irregularity in the security systems of the database occurs in a government agency or public corporation, it shall be notified to the Citizen's Advocate Office, which shall assume jurisdiction. For this purpose, the Citizen's Advocate shall designate a Specialized Advocate who shall</p>	<p>The notice of breach of the security of the system shall be submitted in a clear and conspicuous manner and should describe the breach of the security of the system in general terms and the type of sensitive information compromised. The notification shall also include a toll free number and an Internet site for people to use in order to obtain information or assistance.</p> <p>To notify the citizens the entity shall have the following options: (1) Written direct notice to those affected by mail or by authenticated electronic means according to the Digital Signatures Act. (2) When the cost of notifying all those potentially affected according to subsection (1) of this section or of identifying them is excessively onerous due to the number of persons affected, to the difficulty in locating all persons or to the economic situation of the enterprise or entity; or whenever the cost exceeds one hundred thousand dollars (\$100,000)</p>	<p>[Substitute Notice will include] the following two (2) steps: (a) Prominent display of an announcement to that respect at the entities premises, on the web page of the entity, if any, and in any informative flier published and sent through mailing lists both postal and electronic, and (b) a communication to that respect to the media informing of the situation and providing information as to how to contact the entity to allow for better follow-</p>	<p>Violation of the security system.-- Means any situation in which it is detected that access has been permitted to unauthorized persons or entities to the data files so that the security, confidentiality or integrity of the information in the data bank has been compromised; or when normally authorized persons or entities have had access and it is known or there is reasonable suspicion that they have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information. This includes both access to the</p>

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		said information of any violation of the system's security that has allowed access to those files to unauthorized persons.	code that may have been assigned. (4) Names of users and passwords or access codes to public or private information systems. (5) Medical information protected by the HIPAA. (6) Tax information. (7) Work-related evaluations. Neither the mailing nor the residential address is included in the protected information or information that is a public document and that is available to the citizens in general.		address these types of cases.	or the number of persons exceeds one hundred thousand [(100,000)], the entity shall issue the notice through [substitute notice].	up. When the information is of relevance to a specific professional or commercial sector, the announcement may be made through publications or programming of greater circulation oriented towards that sector.	data banks through the system and physical access to the recording media that contain the same and any removal or undue retrieval of said recordings. Entity.-- Means every agency, board, body, examining board, corporation, public corporation, committee, independent office, division, administration, bureau, department, authority, official, instrumentality or administrative organism of the three branches of the Government; every corporation, partnership, association, private company or organization authorized to do business or operate in the Commonwealth of Puerto Rico; as well as every public or private educational institution, regardless of the level of education offered by it.
Virgin Islands	14 V.I. Code § 2201 et seq.	<i>Territory Agency:</i> 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 the Virgin Islands whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	<i>Territory Agency:</i> 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. (3) Account number, credit or debit card number, in combination with any required	<i>Territory Agency:</i> The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	<i>Territory Agency:</i> Notwithstanding subsection (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.	<i>Territory Agency:</i> 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 \$100,000, or that the affected class of subject persons to be notified exceeds 50,000, or the agency does not have sufficient contact information.	<i>Territory Agency:</i> 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 territory-wide	<i>Territory Agency:</i> 'Personal identification document' means a birth certificate, a drivers license, a state identification card, a public, government, or private employment identification card, a Social Security card, a firearm owner's identification card, a credit card, a debit card, or a passport issued to or on behalf of a person other than the offender, or any document made or issued, or falsely purported to have been

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		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. <i>Commercial entity:</i>	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 territorial government records. <i>Commercial Entity:</i>	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 must be made after the law enforcement agency determines that it will not compromise the investigation. <i>Commercial Entity:</i>	<i>Commercial Entity:</i> Notwithstanding subsection (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 subchapter is 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.	<i>Commercial Entity:</i> 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 \$100,000 or that the affected class of subject persons to be notified exceeds 50,000, or the person or business does not have sufficient contact information.	media. <i>Commercial Entity:</i> 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 territory-wide media.	made or issued, by or under the authority of the United States Government, the Government of the Virgin Islands, or any other state political subdivision of any state or territory, or any other governmental or quasi-governmental organization that is of a type intended for the purpose of identification of an individual, or any such document made or altered in a manner that it falsely purports to have been made on behalf of or issued to another person or by the authority of one who did not give that authority. 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 agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure. <i>Commercial Entity:</i> For purposes of this section, 'breach of the security of the
		Any person or business that conducts business in the Virgin Islands, 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 the Virgin Islands whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	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. (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.	The disclosure must 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. 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.				
		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						

Current as of August 10, 2012

State	Code Citation	Breach Trigger	Information Covered	Timing for notification	Exceptions to Notification	Notification Methods	Optional Public/ Substitute Notification	Some Definitions
		unauthorized person.						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.

Current as of August 10, 2012

201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH

Section:

17.01: Purpose and Scope

17.02: Definitions

17.03: Duty to Protect and Standards for Protecting Personal Information

17.04: Computer System Security Requirements

17.05: Compliance Deadline

17.01 Purpose and Scope

(1) Purpose

This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of this regulation are to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

(2) Scope

The provisions of this regulation apply to all persons that own or license personal information about a resident of the Commonwealth.

17.02: Definitions

The following words as used herein shall, unless the context requires otherwise, have the following meanings:

Breach of security, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Electronic, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Encrypted, the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

Owens or licenses, receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person, a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

Personal information, a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Record or Records, any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Service provider, any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation.

17.03: Duty to Protect and Standards for Protecting Personal Information

(1) Every person that owns or licenses personal information about a resident of the Commonwealth 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 (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

(2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

(a) Designating one or more employees to maintain the comprehensive information security program;

(b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:

1. ongoing employee (including temporary and contract employee) training;
2. employee compliance with policies and procedures; and
3. means for detecting and preventing security system failures.

(c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.

(d) Imposing disciplinary measures for violations of the comprehensive information security program rules.

(e) Preventing terminated employees from accessing records containing personal information.

(f) Oversee service providers, by:

1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and
2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 17.03(2)(f)(2) even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.

(g) Reasonable restrictions upon physical access to records containing personal information,, and storage of such records and data in locked facilities, storage areas or containers.

(h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.

(i) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

(j) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

17.04: **Computer System Security Requirements**

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a

security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:

- (1) Secure user authentication protocols including:
 - (a) control of user IDs and other identifiers;
 - (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
 - (c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
 - (d) restricting access to active users and active user accounts only; and
 - (e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
- (2) Secure access control measures that:
 - (a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
 - (b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;
- (3) Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.
- (4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;
- (5) Encryption of all personal information stored on laptops or other portable devices;
- (6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.
- (7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
- (8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

17.05: Compliance Deadline

- (1) Every person who owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00 on or before March 1, 2010.

REGULATORY AUTHORITY

201 CMR 17.00: M.G.L. c. 93H