502 Leading the Way in Privacy & Data Security Compliance

J. Michael De Janes
General Counsel
ChoicePoint Inc.

Lynn Goodendorf
Vice President, Information Privacy Protection
Intercontinental Hotels Group

Richard Hagerty
Partner
Troutman Sanders LLP

John Hutchins
Partner
Troutman Sanders LLP

Faculty Biographies

J. Michael De Janes
General Counsel
ChoicePoint Inc.

Lynn Goodendorf

Lynn Goodendorf is the global head of data privacy for InterContinental Hotels Group PLC of the United Kingdom with over 3,500 hotels distributed across 100 countries and territories. IHG brands include: InterContinental®, Crowne Plaza®, Hotel Indigo™, Holiday Inn®, Holiday Inn Express®, Staybridge Suites® and Candlewood Suites® along with the world's largest hotel loyalty program, Priority Club® Rewards. Ms. Goodendorf's responsibilities for the company wide privacy program include policies, monitoring and assessments for legal compliance, corporate and hotel communication and training programs, and responses to internal and external inquiries or complaints.

Ms. Goodendorf has prior experience in IT security and network management. Her previous employers include Equifax, Inc. and AT&T. Ms. Goodendorf holds two certifications. She is certified as a information privacy professional (cipp) and a certified information systems security professional (cissp).

Ms. Goodendorf is a member of the International Association of Privacy Professionals (IAPP) and the Information Systems Security Association (ISSA). She co-chairs the IAPP KnowledgeNet for Atlanta and has been a volunteer instructor for CISSP study groups in ISSA. Ms. Goodendorf serves on the board of the Georgia E-Commerce Association and is board vice-chair at Inner Harbour Hospital, a non-profit children's hospital for psychiatric care.

Ms. Goodendorf holds a B.S. degree from St. Cloud State University in Minnesota.

Richard Hagerty

Richard Hagerty is a partner of Troutman Sanders LLP in the Tysons Corner, Virginia office. There he practices in the complex litigation and bankruptcy practice groups and is a member of the privacy and data security team. He regularly represents corporate and other clients in the federal and state courts of Virginia, Maryland and the District of Columbia, and in the bankruptcy courts of these and other jurisdictions.

Prior to joining Troutman Sanders Mr. Hagerty was a principal at Miles & Stockbridge in Rockville, Maryland. Immediately following his graduation from law school he was a law clerk for the Honorable Irma S. Raker of the Circuit Court for Montgomery County, Maryland.

Mr. Hagerty is a member of the character committee for the 7th appellate circuit of Maryland, a volunteer mediator in the D.C. Superior Court, and regularly does pro bono legal work through or on behalf of various non-profit legal services organizations. He has been a frequent lecturer on various legal issues, and also was a co-author of Debtor-Creditor Issues in the Small Law Department Practitioners' Manual published by ACC press.

Mr. Hagerty received his B.A. with honors from Michigan State University and his J.D. with honors from the George Washington University Law School.

John Hutchins

John Hutchins is a partner in the Atlanta office of Troutman Sanders. He represents businesses in various types of commercial disputes and transactions, with particular focus on information technology and intellectual property, including computer hardware and software development projects; government procurement; protection of trade secrets and proprietary business information; e-commerce; licensing and infringement; restrictive covenants; and privacy and data security. He has served as lead counsel in numerous jury trials and bench trials in state and federal courts, as well as arbitration and mediation proceedings.

Mr. Hutchins is the leader of the privacy & data security practice team at Troutman Sanders. He regularly advises clients on issues such as data aggregator liability, state and federal data breach notification laws and regulations, message board misconduct and internet anonymity, website spoofing, privacy policies, the Gramm-Leach-Bliley Act, the Fair and Accurate Credit Transactions Act, the Children's Online Protection Act, Canadian and EU data protection laws, and document retention and destruction. He speaks nationally on issues related to intellectual property, technology, data security and privacy, and he has been published in periodicals such as CIO Magazine, CSO Magazine, ComputerWorld and Cyberspace Lawyer.

He currently serves as the vice chair of the technology law section of the State Bar of Georgia and is the Programs Co-Chair of the intellectual property litigation committee, litigation section, ABA.

He received both his undergraduate and his law degree from the University of South Carolina.

Privacy-Related Provisions of the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005

Richard E. Hagerty*
Troutman Sanders LLP

The Bankruptcy Abuse Prevention and Consumer Protection Act of 2005, 109 P.L. 8, 119 Stat. 23, April 20, 2005 ("BAPCPA"), was the most comprehensive revision of the United States Bankruptcy laws since 1978. While the most notable changes enacted by the law relate to bankruptcies filed by individual consumers, there are numerous provisions affecting business bankruptcies. The BAPCPA also contains several provisions explicitly and implicitly affecting the privacy of personal data in the bankruptcy context. An understanding of these provisions and how they could impact a company's compliance with data security requirements is essential for the general counsel who is attempting to navigate his or her client through the dark waters of the increasingly complicated world of data security compliance.

INTRODUCTION

Ensuring the security of confidential data on consumers has become a fact of life for many American corporations, as has dealing with the negative publicity and potential civil liability of security breaches. A growing number of states and localities have enacted laws designed to provide timely notice to consumers when their confidential personal information is compromised, and the federal government is considering similar measures.[1] One effort that the Congress has already undertaken is to implement certain privacy protections into the Bankruptcy Code, through the bankruptcy changes enacted with the passage of the BAPCPA in 2005.

There are four major areas in the BAPCPA in which the Congress has attempted to insert privacy protections into the Bankruptcy Code.

1. Confidentiality of Consumer Information. Amended Section 363(b)(1) restricts the sale of Personally Identifiable Information ("PII") in possession of a debtor if the debtor has a policy prohibiting or restricting the transfer of PII which was disclosed to consumers and in effect on the petition date.

2. Confidentiality of Healthcare Business Records. Amended Section 351 requires the trustee or debtor-in-possession to destroy confidential patient records of a debtor that is a health care business if it becomes too expensive to maintain the records.

3. Restrictions on Disclosure of Names of Minor Children and Means of Identification. New Section 112 restricts the disclosure of the names of minor children in publicly-filed bankruptcy papers, while amended Section 107 provides protection from the disclosures of certain identifying information affecting individuals.

4. Access of Unsecured Creditors to Information. Amended Section 1102 now requires an unsecured creditor's committee to provide access to information to creditors that hold claims of the kind represented by the committee and who are not members of the committee.

It is not difficult to imagine scenarios in which one or more of these provisions could affect an American corporation. Imagine, for instance, that you are the general counsel of an online retailer. Your client sells a variety of products and compiles and maintains a large and evolving database of personal information concerning its customers. The company has a privacy policy that prohibits the sale or other transfer of such information without the customer's explicit consent. Due to increasing competition and increasing costs the client is in financial difficulty, and the CEO comes to you for advice on whether to file for Chapter 11 reorganization in an effort to restructure the company's business, shed some product lines, and streamline operations. One of the most valuable assets that the company has is its database of consumer information. Can the company file for bankruptcy and sell a portion of its online business (including its customer database) in an effort to raise cash to reorganize its remaining operations?

As you consider the CEO's questions you must factor into your analysis the fact that the company employs 1,500 people, and that 100 of them are obliged to make payments on child support orders through wage garnishments that are withheld from employees' paychecks and remitted directly to state child support enforcement agencies by the company's payroll department. Do the state agencies and beneficiaries of such payments need to be notified of a bankruptcy filing? Does the company need to disclose any payments made on account of such child support orders in the schedules of assets and liabilities and/or statement of financial affairs that will have to be filed in the case? Assuming that the answer to both of these questions is "yes," are there any limitations on the types of information that can be disclosed in the public filings regarding such payments?

No lawyer wants to create new law in a situation where the courts could ultimately rule against counsel's advice, to the detriment of the client. However, with the relative nascence of the privacy changes enacted by the BAPCPA and the dearth of judicial interpretation, the general counsel now faces the unenviable task of advising his/her client on how to comply with the statute with little or no guidance. The following analysis is an attempt to summarize the key provisions of the BAPCPA affecting privacy of personal data, to highlight the provisions of greatest significance, and to provide some practical suggestions for applying these provisions in practice. Each of these changes has practical implications for companies that are contemplating a bankruptcy filing. In addition, two of the changes – dealing with PII and creditor access to information – can

* The author would like to acknowledge the assistance of Erin O'Neil, J.D. candidate, the George Washington University (class of 2007), for her research and assistance on these materials.
[1] *See* "Congress Proposes Data Breach Notification Law," CSO Online, July 24, 2006, available at http://www2.csoonline.com/blog_view.html?CID=23257&source=csonewswatch.

impact non-debtor companies that have either pre- or post-petition dealings with a bankrupt.

ANALYSIS

I. CONFIDENTIALITY OF CONSUMER INFORMATION

The provisions of the BAPCPA that most directly affect data security compliance are those dealing with so-called "personally identifiable information," confidential information collected from consumers and maintained by a debtor pursuant to a privacy policy in effect before the filing of a bankruptcy case. Although these provisions have important implications for any company that collects confidential data from its consumer customers, they have received virtually no judicial scrutiny since the BAPCPA was enacted. For this reason alone an understanding of these provisions is essential for the general counsel who represents either a company that is considering filing for bankruptcy protection, or considering purchasing assets from a company that is already in bankruptcy.

A. Personally Identifiable Information Defined

The BAPCPA places new restrictions on the sale of Personally Identifiable Information ("PII") in possession of the debtor if the debtor had disclosed a privacy policy to consumers that was still in effect on the petition date.[2] New Section 101(41A)(A) of the Bankruptcy Code defines PII as information "provided by an individual to the debtor in connection with obtaining a product or a service from the debtor primarily for personal, family, or household purposes" and includes the name, residence address, electronic address, telephone number, social security number, and credit card number.[3] Subsection (B) further provides that PII also includes a birth date, birth certificate or adoption number, and place of birth, or "any other information concerning an identified individual that, if disclosed, will result in contacting or identifying such individual physically or electronically," if this information is identified in connection with one of the items listed under Section 101(41A)(A).[4] This definition is at least as broad as the definition of "personal information" in the California Security Breach Information Act,[5] the model for many state data breach notification statutes.

B. New Restrictions on Sale of Personally Identifiable Information

Amended Section 363(b)(1) restricts the sale of PII in possession of the debtor *if* the debtor has a policy prohibiting the transfer of PII that was disclosed to consumers and in effect on the petition date.[6] Section 363(b)(1) does not apply, however, if the debtor did not have a policy in effect on the petition date. When a debtor has a policy prohibiting the sale or transfer of PII, that PII may only be sold or leased as an incident of a Section 363 asset sale if one of the following conditions is met:

> (A) such sale or such lease is consistent with such policy; or
> (B) after appointment of a consumer privacy ombudsman in accordance with section 332, and after notice and a hearing, the court approves such sale or such lease--[7]

When making a decision regarding the transfer of PII, the court considers the individual facts, circumstances, and conditions of the transfer, and the court must find that there was no showing that the transfer would violate applicable nonbankruptcy law.[8]

New Section 332 sets forth the procedure for appointing a consumer privacy ombudsman ("CPO"). The CPO must be appointed at least five days before the hearing on whether or not PII should be sold or transferred, and the CPO must be a disinterested person other than the United States Trustee. The CPO may be compensated from the bankruptcy estate pursuant to amended Section 330(a). The role of the CPO is to advise the court on whether or not the court ought to authorize the sale of PII. The CPO's assessment may be based upon the following:

> (1) the debtor's privacy policy;
> (2) the potential losses or gains of privacy to consumers if such sale or such lease is approved by the court;
> (3) the potential costs or benefits to consumers if such sale or such lease is approved by the court; and
> (4) the potential alternatives that would mitigate potential privacy losses or potential costs to consumers.[9]

The CPO is prohibited from disclosing any PII obtained during this process.[10] The statute provides no minimum professional qualifications for the position of CPO. Interim Bankruptcy Rule 6004(g) requires that a motion for authority to sell or lease PII include a request for an order directing the appointment of a CPO,[11] and Interim Bankruptcy Rule 2002(c)(1) requires that the motion contain a statement regarding whether the proposed sale or lease is consistent with the company's policy prohibiting the transfer of PII.[12]

---

[2] 11 U.S.C. § 363(B)(1).
[3] 11 U.S.C. § 101 (41A)(A).
[4] 11 U.S.C. § 101 (41A)(B).
[5] Cal. Civ. Code § 1798.82(e).
[6] 11 U.S.C. § 363(B)(1).
[7] *Id.*
[8] *Id.*
[9] 11 U.S.C. § 332(b).
[10] 11 U.S.C. § 332(c).
[11] Fed. R. Bankr. Proc. 6004(g) (Interim Amend. 2005).
[12] Fed. R. Bankr. Proc. 2002(c)(1) (Interim Amend. 2005).

C. Commentary On New Provisions Regarding The Confidentiality Of Consumer Information

Congress intended the new restrictions on the sale of PII to enhance privacy protections for individuals who have provided PII to companies that ultimately file for bankruptcy. Some commentators have expressed concern that the BAPCPA will not protect PII to the degree that Congress intended.[13] Commentators are especially concerned with new Section 332's failure to grant adequate authority to CPOs, as well as the lack of any criteria (other than disinteredness) for the appointment of a CPO.[14] In addition, because the statutory language confines the CPO's responsibilities under Section 332 to review of the "debtor's privacy policy," a narrower term than the debtor's "policy prohibiting the transfer of personally identifiable information," which is used in Section 363(b)(1), commentators have expressed the concern that the new law could be interpreted to prevent CPOs from examining other relevant policies, such as the debtor's personal data protection policy, that may contain representations and warranties regarding PII protection.[15]

Another concern is the statute's failure to set forth any professional qualifications for a CPO.[16] The trustee, not the court, appoints the CPO, which some commentators view as an inherent conflict of interest. Roland Trope and Michael Power argue that an appointed CPO should have privacy expertise as well as expertise in "cross-border privacy issues (including knowledge and understanding of applicable laws in countries from which the personally identifiable data were obtained or to which they might be transferred)" to ensure that the CPO can provide information and analysis needed by the court to determine potential risks for loss of privacy.[17]

The statute also does not set forth any criteria for evaluating the potential losses or gains of privacy to consumers.[18] Trope and Power offer the following suggestion:

> [T]he appropriate privacy protective metrics for a bankruptcy court to consider (and for the privacy ombudsman to bring to a bankruptcy court's attention) should include those that a responsible sophisticated company would probably require in an outsource agreement or in a data governance agreement if such agreement involved the transfer of sensitive data from such company to its offshore outsource vendor. A bankruptcy court, in exercise of its discretion, should be reluctant to approve a section 363(b)(1) "sale or lease" that would result in a transfer of personally identifiable data to any entity whose data governance is demonstrably deficient, contains material weaknesses, or for any other reason is more than marginally inferior to the debtor's data governance.[19]

Trope and Power also note, however, that the statute fails to give the CPO the power to subpoena documents or file a motion to seek the production of documents.[20] Therefore, the CPO may not be able to obtain the information from the debtor or other sources that is necessary to determine the potential privacy losses or gains from a proposed sale or lease of PII.

Even if the CPO is able to obtain the requisite documents, he or she may not have enough time to thoroughly review them, because Section 332 only requires that a CPO appointment be made not less than *five days* before the hearing on the proposed sale of PII. Five days is almost certainly an insufficient amount of time within which to review information and determine what privacy losses or gains may result from a sale or lease of PII.

> Five days notice is meager and insufficient for any ombudsman to prepare to fulfill their duties in a hearing involving a potentially complex bankruptcy, and, moreover, involving potentially millions of hard copy and electronic records containing "personally identifiable information" that may have been obtained from numerous foreign jurisdictions, each with its own potentially applicable privacy and personal data protection laws and regulations.[21]

Other commentators are more optimistic, and believe that courts will allow enough time between appointing the CPO and holding the hearing to ensure the CPO will give the court well-researched information and recommendations.[22] Unfortunately, there has thus far been no reported decision of the bankruptcy courts providing any guidance on this issue.

Some commentators have suggested that companies will take action in light of the BAPCPA to review and revise their privacy policies to allow for the transfer of PII in bankruptcy proceedings.[23] Legal counsel for some lending institutions are also recommending that lenders "analyze the value of customer lists and databases and review potential borrowers' privacy policies in order to craft loan documents that contemplate the application of new Section 363(b)(1) in the event of bankruptcy,"[24] suggesting thereby that lenders preserve to themselves the right to sell PII without complying with

---

[13] Roland L. Trope & E. Michael Power, Cyberspace Law: Lessons in Data Governance: A Survey of Legal Developments in Data Management, Privacy and Security, 61 BUS. LAW. 471, LEXSEE 61 BUS LAW 471, at 25 (2005).
[14] *Id.* at 23.
[15] *Id.* at 24.
[16] *Id.* at 23.
[17] *Id.* at 25.
[18] *Id.* at 24.
[19] *Id.* at 24.
[20] *Id.* at 24.
[21] *Id.* at 23.
[22] John J. Sparacino & C. John Melissinos, *Overview of New Provisions on Sale of Personally Identifiable Information,* ABI COMMITTEE NEWS (Am. Bankr. Inst., Alexandria, Va.), July 2005 *available at* http://abiworld.net/newsletter/assetsales/vol2num2/OverviewofNewProvisions.pdf.
[23] *See Additional Highlights of the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA)*, CREDITOR'S RIGHTS QUARTERLY, BANKRUPTCY GROUP NEWSLETTER (Shipman & Goodwin LLP) December 2005, http://www.shipmangoodwin.com/publications/Newsletters/creditors_rights_q4.pdf.
[24] *Id.*

the debtor's privacy policy in the event of a forced sale following a bankruptcy filing. These trends, taken together with the issues discussed above, do little to clarify the degree of protection the BAPCPA will actually provide for PII.

D. Practical Impact of Restrictions on the Sale of PII

Because "[t]he modern trend in chapter 11 [bankruptcies] is to liquidate the business as a going a [*sic*] concern through a sale under section 363,"[25] the restrictions on the sale of PII imposed by the BAPCPA have the potential to affect the going concern value of a bankrupt company's assets. This could be particularly true of companies in industries that routinely collect and use PII – for instance, airlines, online retailers, and other companies that sell goods or services directly to the consuming public and facilitate those sales through the collection of confidential information on their customers. Since such companies almost routinely adopt and publish privacy policies (and may use them in their promotional advertising), it is increasingly likely that financially troubled companies in such industries will be faced with the choice of jettisoning or amending their policies prior to filing for bankruptcy, or dealing with restrictions imposed by such policies when they attempt to sell their assets after a bankruptcy filing. Similarly, the purchasers of such assets – often competitors in the same industries – can be expected to factor in the cost and potential delay of dealing with CPO appointment and review into the price they are willing to pay for their bankrupt competitor's assets, particularly if those assets include PII on the bankrupt's customers. Indeed, there are almost certainly industries and companies for which the confidential PII could be one of the more valuable assets, since it provides a purchaser of those assets with ready-made access to a wealth of information on potential customers.

While the theory behind the restrictions on the sale of PII – to protect against the untoward disclosure of PII in the context of a Section 363 asset sale – creates the possibility of depressing the going concern value of bankrupt companies seeking to dispose of PII in their possession, it remains to be seen whether the application of new Section 363(b) will have that effect. If, as has been suggested by some commentators, the criteria and procedure for appointing a CPO are inadequate to protect consumers from the untoward disclosure of their PII, then new Section 363(b) is unlikely to do more than add a small amount of time and some additional expense to the process of handling asset sales in bankruptcy. When one considers that one of the primary purposes of the bankruptcy system is to maximize recovery for creditors, such a result would not be surprising. If, on the other hand, bankruptcy courts take seriously Congress' intention to protect PII, then it is possible that revised Section 363(b) could impact the asset sale process by forcing all participants in the process – the debtor, the committee, the secured creditors, the potential buyers, and the court – to evaluate whether the sale or lease of PII is consistent with a debtor's existing privacy policy, and if not, whether there are adequate safeguards for protecting against the untoward disclosure of PII built-into the proposed sale. Because there have been no reported decisions dealing with Section 363(b), only time will tell how it will affect the bankruptcy process.

[25] Hon. Michael G. Williamson, *Complex Chapter 11 Developments*, 11th Annual Southeast Bankruptcy Workshop (Am. Bankr. Inst., Alexandria, Va.), July, 2006.

In the interim, however, general counsel for companies that possess PII and are considering filing for bankruptcy protection have three options they can present to their clients. The first option is to jettison the company's privacy policies before filing for bankruptcy, to free the company from the need to comply with Section 363(b)'s restrictions on the sale of PII. Because of the negative publicity and attendant effect on the company's business from such a decision – not to mention potential liability under state privacy statutes – this option is not attractive.

The second option that the general counsel of a financially troubled company can present to his or her management is to amend the company's existing privacy policy to permit the sale or other transfer of PII in the event of a bankruptcy filing, and pursuant to a court-approved asset sale. While this option is probably less traumatic that the first option, it presents many of the same risks.

The third option, and the one that holds the most promise, is to embrace the BAPCPA's restrictions on the sale of PII. By conditioning any bankruptcy sale of PII on court approval pursuant to Section 363(b)(1), the general counsel of an insolvent company may be best able to protect his or client from the negative implications of the sale of PII. Companies that elect this option should cooperate with the United States Trustee to ensure that a CPO is selected who has both the business acumen and the knowledge of privacy law sufficient to provide a credible analysis to the bankruptcy court. When filing its motion to approve bid procedures and/or a sale of assets that includes PII the debtor should request that the court appoint a CPO sufficiently far in advance of the proposed sale to enable the CPO to adequately review all factors described under Section 332(b), *including* the debtor's policy prohibiting the transfer of PII. The debtor ought to provide the CPO with access to information sufficient to conduct his or her analysis (subject to an appropriate confidentiality order). Most importantly, the debtor ought to structure its proposed sale of PII to either comply with its existing privacy policies or, if those policies prohibit the sale of PII, to protect against the misuse or untoward disclosure of PII by the purchaser. The financially troubled company that elects this third option may find that the additional time and cost involved in the sale of PII is more than offset by the increased assurance that such a sale will not generate lawsuits by disgruntled consumers or a related backlash in the marketplace.

II. RESTRICTIONS ON ACCESS TO AND DESTRUCTION OF CONFIDENTIAL PATIENT RECORDS IN HEALTH CARE BUSINESSES

Apart from the protections afforded for Personally Identifiable Information, which apply to any company that files for bankruptcy and seeks to sell assets that include PII, the BAPCPA has created a new category of debtors as to which specific restrictions on the disposal of confidential information will now apply. These restrictions apply to "health care businesses," which are newly-defined by the BAPCPA, and as to which Congress has determined that there was a need to provide specific instruction. While ensuring patient privacy is not the primary focus of the new provisions on health care

businesses, the new law contains explicit and implicit privacy provisions that must be consulted by any practitioner who represents or is dealing with a health care business that has filed or is contemplating a bankruptcy filing.

A. Health Care Businesses Defined

New Bankruptcy Code Section 101(27A) defines "health care business" to include any public or private entity (for-profit and non-profit) that is "primarily engaged in offering to the general public facilities and services for . . ." health care. Health Care Businesses include hospitals, nursing homes, ambulatory, emergency and urgent care facilities, hospices, and home health agencies.[26]

B. New Provisions Regarding Health Care Businesses and Confidentiality

New Code Section 351 requires the trustee or debtor-in-possession to destroy confidential patient records of a health care business debtor if the cost of maintaining the records becomes too expensive. This section applies when the trustee does not have sufficient funds to pay for the storage of patient records. The trustee must take the following actions before destroying any records:

- The trustee must publish notice in at least one "appropriate newspaper"[27]
- During the 180 days after notice, the trustee must attempt to notify patients and their health insurance providers directly by sending notification to the most recent mailing address[28]
- 365 days after notification, the trustee shall mail via certified mail a written request to appropriate Federal agencies, requesting permission to deposit unclaimed patient records with that agency

If a Federal agency does not accept a request to deposit records with it, the trustee shall destroy the unclaimed records. If the records are written, the statute requires them to be shredded or burned.[29] Magnetic, optical, or other electronic records must be destroyed in a way so they "cannot be retrieved."[30] Interim Bankruptcy Rule 6011 requires certification of record destruction (including what method was used for destruction) within 30 days after the records have been destroyed.[31]

New Bankruptcy Code Section 333 requires the court to appoint a patient care ombudsman within 30 days of filing any bankruptcy case by or against a health care business.[32] Patient care ombudsmen are required to receive court approval before reviewing patient records; once such approval is granted, patient care ombudsmen are required to maintain the confidentiality of patient records.[33] The courts are also able to place restrictions on patient care ombudsmen to further protect patients' privacy.[34]

C. Practical Implications of the New Rules on Health Care Bankruptcies

There have been no reported cases applying or otherwise discussing new Sections 351 and 333, and the principal focus of commentary on the new provisions has been to summarize them.[35] For this reason, it is probably too soon to know how the BAPCPA will affect the health care industry's compliance with the privacy obligations imposed by various provisions of federal and state law. It remains to be seen, for instance, whether the provisions of new Code Section 351 requiring the destruction of confidential patient records are in conflict with competing standards and restrictions under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),[36] which generally requires adoption of security standards to protect against the disclosure of "individually identifiable health information."[37] In addition, it is unclear to what extent a patient care ombudsman will have authority to monitor a health care business debtor's compliance with HIPAA and other privacy restrictions, a fact which means that the general counsel of a bankrupt health care business should not rely upon the patient care ombudsman to monitor such compliance.

In this regard it bears noting that subsection (c)(1) of Section 333 imposes restrictions on the patient care ombudsman's access to and review of confidential patient records.[38] In one recent case under the BAPCPA the patient care ombudsman appointed by the Bankruptcy Court was required to seek emergency approval for review of confidential patient records in order to perform her statutory duties.[39] The Court only granted such approval after providing for notice to the affected patients, and specifically ordered the ombudsman to "keep and maintain all patient information she reviews confidential in accordance with both 11 U.S.C. § 333(c) and applicable nonbankruptcy law."[40]

---

[26] 11 U.S.C. § 101(27A).
[27] The statute does not require that more than one notice be published, something that calls into question the efficacy of the publication requirement. *See* 11 U.S.C. § 351(1)(A).
[28] Interim Bankruptcy Rule 6011 requires court approval of notice of the intended destruction of records, and specifies the required content of the notice. Fed. R. Bankr. Proc. 6011 (Interim Amend. 2005).
[29] 11 U.S.C. § 351(3)(A).
[30] 11 U.S.C. § 351(3)(B).
[31] Fed. R. Bankr. Proc. 6011(d) (Interim Amend. 2005).
[32] 11 U.S.C. § 333(a).
[33] *Id.* (A patient care ombudsman "shall have access to patient records consistent with authority of such ombudsman under the Older Americans Act of 1965 and under non-Federal laws governing the State Long-Term Care Ombudsman program.").
[34] 11 U.S.C. § 333(c)(1).
[35] *See, e.g.*, William W. Kannel & Sara R. Bollerup, *Impact of the New Bankruptcy Law on Health Care Bankruptcies*, Health Care Committee Newsletter Vol. 2, No. 2 (Am. Bankr. Inst., Alexandria, Va.), April, 2005, available at http://abiworld.net/newsletter/healthcare/vol2num2/impact.html.
[36] 104 P.L. 191, 110 Stat. 1936, August 21, 1996.
[37] 42 U.S.C. §§ 1320d, *et seq*.
[38] 11 U.S.C. § 333(c)(1).
[39] *See* Emergency Motion by Patient Care Ombudsman for Order Approving Review of Confidential Patient Records Pursuant to 11 U.S.C. § 333, *In re Atlantic Health Services, Inc.*, Case No. 06-10356 (PM), Docket No. 69 (Bankr. Ct. D. Md., March 9, 2006).
[40] Order Granting Motion for Reconsideration and Approving Review by Patient Care Ombudsman of Confidential Patient Records Pursuant to 11 U.S.C. § 333(c), *In re Atlantic Health Services, Inc.*, Case No. 06-10356 (PM), Docket No. 83 (Bankr. Ct. D. Md., March 17, 2006).

III. RESTRICTIONS ON DISCLOSURE OF NAMES OF MINOR CHILDREN AND MEANS OF IDENTIFICATION

New Section 112 restricts the disclosure of the names of minor children in publicly-filed bankruptcy papers,[41] while amended Section 107 provides protection from the disclosures of certain identifying information affecting individuals.[42] Both sections restrict access to what is otherwise public information in bankruptcy filings for the purpose of protecting the privacy of individuals. The latter section in particular creates a tension between protecting individual's privacy expectations and other provisions of the BAPCPA that require the disclosure by debtors of more detailed information regarding their federal income taxes.

New Bankruptcy Code Section 112 provides as follows:

§ 112. Prohibition on disclosure of name of minor children

> The debtor may be required to provide information regarding a minor child involved in matters under this title but may not be required to disclose in the public records in the case the name of such minor child. The debtor may be required to disclose the name of such minor child in a nonpublic record that is maintained by the court and made available by the court for examination by the United States trustee, the trustee, and the auditor (if any) serving under section 586(f) of title 28, in the case. The court, the United States trustee, the trustee, and such auditor shall not disclose the name of such minor child maintained in such nonpublic record.

The legislative history for this section indicates that Congress was concerned about protecting the identity of the debtor's minor children.[43] Similarly, new Section 107(c) provides protections from disclosure of certain information "to the extent the court finds that disclosure . . . would create undue risk of identity theft or other unlawful injury to the individual's property." In enacting this provision Congress was similarly concerned about protecting individuals from misuse of their confidential personal information.[44]

§ 107. Public access to papers

> (c) (1) The bankruptcy court, for cause, may protect an individual, with respect to the following types of information to the extent the court finds that disclosure of such information would create undue risk of identity theft or other unlawful injury to the individual or the individual's property:
>
> (A) Any means of identification (as defined in section 1028(d) of title 18) contained in a paper filed, or to be filed, in a case under this title.
>
> (B) Other information contained in a paper described in subparagraph (A).
>
> (2) Upon ex parte application demonstrating cause, the court shall provide access to information protected pursuant to paragraph (1) to an entity acting pursuant to the police or regulatory power of a domestic governmental unit.
>
> (3) The United States trustee, bankruptcy administrator, trustee, and any auditor serving under section 586(f) of title 28 –
>
> (A) shall have full access to all information contained in any paper filed or submitted in a case under this title; and
>
> (B) shall not disclose information specifically protected by the court under this title.

While both of these provisions would seem to be relevant only to individual bankruptcy cases, the reality is that businesses that have filed for bankruptcy since the effective date of the BAPCPA have been forced to deal with the restrictions imposed by Sections 112 and 107(c). This is largely due to two facts that operate in tandem to implicate business debtors in the payment of domestic support obligations: the percentage of the population that is implicated in domestic support obligations,[45] and the provisions of the BAPCPA that provide preferred treatment to "domestic support obligations," debts that accrued before or after the filing of a bankruptcy petition and which are in the nature of alimony, maintenance or support and established by separation agreement, divorce decree or other court order.[46] Since domestic support obligations are entitled to favored treatment under the BAPCPA in areas as diverse as the priority of claims,[47] the conditions for confirmation of a Chapter 11 plan of reorganization,[48] and whether or not pre-petition payments made on account of domestic support obligations are recoverable as preferences,[49] it is likely that even business debtors filing Chapter 11 and 7 cases will have to disclose information concerning such obligations, and send notices to the beneficiaries of them. Because such information will often, if not always, include the names and other identifying information regarding both the obligors under and beneficiaries of such obligations – many of who may be children – business debtors

[41] 11 U.S.C. § 112.
[42] 11 U.S.C. § 107.
[43] House Report No. 109-31 (Part I), p. 21, available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_reports&docid=f:hr031p1.109.pdf.
[44] *Id.*

[45] One Chapter 13 trustee practicing in the Eastern District of Virginia has estimated that approximately 30%-33% of his Chapter 13 case load includes cases in which DSOs are implicated. *See* August 19, 2006 e-mail from Frank J. Santoro, Marcus, Santoro & Kozak, P.C., to Richard E. Hagerty, Troutman Sanders LLP. If this percentage can be extrapolated to the population as a whole, then it is likely that a company facing bankruptcy will be implicated in DSOs, commonly through administering payments pursuant to wage garnishments.
[46] 11 U.S.C. § 101(14A).
[47] 11 U.S.C. § 507(a)(1) provides a first priority for domestic support obligations, subordinate only to certain allowed administrative expenses incurred by chapter 7, 13 or 11 trustees under 11 U.S.C. § 503(b).
[48] 11 U.S.C. § 1129(a)(14) now requires full payment of amounts owed by a debtor under a domestic support obligation both pre-petition and post-petition as a condition of confirmation of a Chapter 11 plan.
[49] Pursuant to 11 U.S.C. § 547(c)(7) prohibits the recovery as a preference of "a bona fide payment of a debt for a domestic support obligation."

will have to be particularly vigilant not to disclose information in violation of Sections 107(c) and 112.[50]

New Section 107(c) also creates a tension with other provisions of the BAPCPA that require individual debtors filing under Chapters 7, 11 or 13 to provide copies of their federal tax returns to the trustee and to creditors who request them,[51] and in some cases to file them with the court.[52] Section 315(c) of the BAPCPA required the Director of the Administrative Office of the United States Courts to establish procedures for safeguarding the confidentiality of such tax information within 180 days of April 20, 2005.[53] In response to this requirement, consumer advocacy groups proposed that the Administrative Office of the Courts impose stringent restrictions on creditor access to, and use of, tax returns.[54] The Director of the Administrative Office of the U.S. Courts responded to BAPCPA Section 315(c) by issuing an interim Guidance on September 2005,[55] which was in turn adopted by the Judicial Conference at its September 20, 2005 meeting.[56] The Director's interim guidance adopted many of the procedures proposed by the Consumer Federation of America and others, including the following:

- No tax information filed with the bankruptcy court or otherwise provided by the debtor will be available to the public via the Internet, PACER, or CM/ECF.
- Debtors providing tax information under 11 U.S.C. § 521 should redact personal information as set forth in the Judicial Conference's Policy on Privacy and Public Access to Electronic Case Files.
- In order to obtain access to debtor's tax information that is filed with the bankruptcy court, the movant must file a motion with the court, which should include a description of the movant's status, a description of the specific tax information requested, a statement indicating that the information cannot be obtained from other sources, and a statement showing a demonstrated need for the information.[57]

[50] Domestic support obligations are not the only types of claims that could implicate the provisions of Section 107(c). To the extent that a business debtor owes pre-petition wages or other benefits to employees, it will be required to disclose identifying information in its schedules of the type that could implicate the restrictions of Section 107(c). *See* 11 U.S.C. § 521(a)(1) *and compare* Fed. R. Bankr. Proc. 1007 *and* Fed. R. Bankr. Proc. 1007 (Interim Amend. 2005). Whether the disclosure of such information "would create undue risk of identity theft or other unlawful injury to the individual [employees] or [their] property" is something that will have to be reviewed on an *ad hoc* basis, with due regard to the type of information to be disclosed.

[51] *See* 11 U.S.C. § 521(e)(2).

[52] *See* 11 U.S.C. § 521(f).

[53] Pub. L. 109-8, Title III, § 315(c), 119 Stat. 91.

[54] Testimony of Travis B. Plunkett on Behalf of the Consumer Federation of America, the National Consumer Law Center and the U.S. Public Interest Research Group, before the Subcommittee on Commercial & Administrative Laws of the House Judiciary Committee, July 26, 2005, at 9-11, available at http://www.abiworld.org/pdfs/s256/Plunkett.pdf.

[55] Director's Interim Guidance Regarding Tax Information Under 11 U.S.C. § 521, September 21, 2005, available at http://www.vaeb.uscourts.gov/files/tax_return_guidance_20050920.pdf.

[56] Report of the Proceedings of the Judicial Conference of the United States, September 20, 2005, at 13, available at http://www.uscourts.gov/judconf/Sept05proc_final.pdf.

IV. UNSECURED CREDITORS' ACCESS TO INFORMATION

The last major privacy-related change enacted by the BAPCPA, and the one that has thus far generated the most litigation, has to do with providing creditor access to information. Section 405(b) of the BAPCPA amended Bankruptcy Code Section 1102(b) to require that creditor's committees and equity security committees appointed pursuant to Bankruptcy Code Section 1102(a) are required "to give creditors having claims of the kind represented by the committee access to information. In addition, the committee must solicit and receive comments from these creditors and, pursuant to court order, make additional reports or disclosures available to them."[58] While the new provisions do not explicitly deal with confidential third-party information in the possession of the debtor, they have the potential to subject such information to access by creditors who would not otherwise be entitled to it. When added to the concerns about avoiding the disclosure of confidential or privileged information about a debtor it is unsurprising that this provision has generated as much litigation as it has.

A. New Provision Regarding Creditor Access

Amended Bankruptcy Code Section 1102, entitled "Creditors' and equity security holders' committees," requires a committee appointed under the section to provide access to information to creditors who hold claims of the kind represented by that committee and who are not appointed to the committee.[59] The statute further requires that the committees "(B) solicit and receive comments from the creditors described in subparagraph (A); and (C) be subject to a court order that compels any additional report or disclosure to be made to the creditors described in subparagraph (A)."[60] This new provision is a significant change from earlier bankruptcy law because committees are now specifically required to provide information to their constituents; before they merely had a fiduciary duty to their constituents that did not affirmatively require the sharing of information.[61]

[57] Director's Interim Guidance, *supra* note 53, at 1-2.

[58] House Report No. 109-31 (Part I), p. 87.

[59] 11 U.S.C. § 1102(b)(3), which provides as follows:

> (3) A committee appointed under subsection (a) shall--
> (A) provide access to information for creditors who--
> (i) hold claims of the kind represented by that committee; and
> (ii) are not appointed to the committee;
> (B) solicit and receive comments from the creditors described in subparagraph (A); and
> (C) be subject to a court order that compels any additional report or disclosure to be made to the creditors described in subparagraph (A).

[60] *Id.*

[61] Maria Ellena Chavez-Ruark, *How Courts are Interpreting the New Duty to Provide Access to Information*, BYLINES (DLA Piper Rudnick Gray Cary) June 2006, available at http://www.dlapiper.com/interpreting_access_to_information/.

B. Developments and Commentary Regarding Creditor Access

Most commentary regarding new Section 1102(b)(3) has criticized the statute for failing to define "information" and how this information should be disseminated.[62] At the heart of this ambiguity is whether committees must disclose confidential information, or information that would normally be protected by privilege or the work product doctrine.[63] Another issue is with whom the committee must share information; for instance, does Section 1102(b)(3) require committees to share information with equity security holders?[64]

Committees formed in cases filed since the effective date of the BAPCPA have sought answers to these questions through Section 1102 clarification motions, in which they have asked courts to specify what kind of information they are required to provide, or whether they are required to provide information at all.[65] However, because the statute provides little guidance, courts have provided protection for confidential and privileged information to varying degrees. At this writing the bankruptcy courts are split on whether "a committee must disclose non-public information and whether individual creditors should be required to execute confidentiality orders."[66]

Some courts have provided protection to confidential information, but have not provided a lot of detail regarding a committee's responsibilities. For instance, in *In re LG.Philips Displays USA, Inc.*, the United States Bankruptcy Court for the District of Delaware concluded that the official committee of unsecured creditors was not authorized or required to provide access to the debtor's privileged or confidential information.[67] The Court did conclude, however, that the committee was permitted (but not required) to allow access to privileged information when the information is not confidential information and the privilege is "held and controlled solely by the committee."[68] The court defined "Confidential Information" to mean:

> any nonpublic information of the Debtor, including, without limitation, information concerning Debtor's assets, liabilities, business operation, projections, analyses, compilations, studies, and other documents prepared by the Debtor or its advisors or other agents, which is furnished, disclosed, or made known to the Committee, whether intentionally or unintentionally and in any manner, including written form, orally or through any electronic facsimile or computer-related communication. Confidential Information shall include (a) any notes, summaries, compilations, memoranda, or similar written materials disclosing or discussing Confidential Information; (b) any written Confidential Information that is discussed or presented orally; and (c) any other Confidential Information conveyed to the Committee orally that the Debtor or its advisors or other agents advise the Committee should be treated as confidential.[69]

The court in the *LG.Philips* case then specifically stated that the following information would not be considered Confidential Information:

> Confidential Information shall not include any information or portions of information that: (i) is or becomes generally available to the public or is or becomes available to the Committee on a non-confidential basis, in each case to the extent that such information became so available other than by a violation of a contractual, legal, or fiduciary obligation to the Debtor; or (ii) was in the possession of the Committee prior to its disclosure by the Debtor and is not subject to any other duty or obligation to maintain confidentiality.[70]

Privileged information was defined as "any information subject to the attorney-client or some other state, federal, or other jurisdictional law privilege (including attorney work product), whether such privilege is solely controlled by the Committee or is a joint privilege with the Debtor or some other party."[71] Significantly, the court did not specifically address whether confidential data about third-parties in the debtor's possess would be "Confidential Information." As described below, a strong argument can be made that such information should be afforded the same level of protection.

The Delaware Bankruptcy Court entered a similar order in the case of *In re FLYi, Inc.*[72] By contrast, in the case of *In re Amcast Automotive of Indiana, Inc.*, the Bankruptcy Court for the Southern District of Indiana did not restrict the committee's ability to disclose either confidential or privileged information, but instead gave the committee the sole discretion to make the determination about whether such information should be disclosed.[73] With respect to confidential information provided by third-parties, the court in *Amcast* conditioned its disclosure on the consent of the third-party.

Other courts have provided extensive detail regarding what information is confidential and privileged, and what procedures committees must use to disseminate such information. For instance, the United States Bankruptcy Court for the Southern

---

[62] *Id.*
[63] *Id.*
[64] Scott Y. Stuart, *Until Courts Set Boundaries, Arbitrariness Will Define New Information-Sharing Rules*, DAILY BANKRUPTCY REVIEW (Dow Jones & Company, Inc.) June 21, 2006, available at http://www.donlinrecano.com/dr201/news/DBR%20Article.pdf.
[65] *See id.*
[66] Chavez-Ruark, *supra* note 61.
[67] Order Clarifying and Providing that the Official Committee of Unsecured Creditors is not Authorized or Required to Provide Access to Confidential Information of the Debtor or to Privileged Information , *In re LG.Philips Displays USA, Inc.*, No. 06-10245, Docket No. 216, at 2 (Bankr. D. Del., March 18, 2006).
[68] *Id.*
[69] *Id.* at n. 2.
[70] *Id.*
[71] *Id.* at n.3.
[72] Order Setting Forth Procedures for Sharing of Information by Creditors Committee, *In re Flyi, Inc.*, Case No. 05-20011, Docket No. 145 (Bankr. D. Del., November 17, 2005).
[73] Order Approving Information Sharing Procedures of Official Committee of Unsecured Creditors, *In re Amcast Automotive of Indiana, Inc.*, Case No. 05-33322, Docket No. 358, at 3 (Bankr. S.D. Ind., March 6, 2006).

District of New York has entered a detailed opinion on the "information" that must be provided to creditors under Section 1102(b). In *In re Refco, Inc.,*[74] the Bankruptcy Court for the Southern District of New York discussed the proper meaning and scope of Section 1102(b)(3), and approved an order establishing a strict protocol for the committee's dissemination of information to creditors. This protocol included the following:

- Establishment and maintenance of an internet-accessed website containing public information the case, including general information, monthly committee reports, highlights of significant events, a calendar of upcoming events, access to claims dockets, nonpublic forms to request "real-time" electronic case information and/or request more detailed, non-public information regarding the debtor;[75]

- Strict limits on the committee's obligation to disseminate without further court order:

  > confidential, proprietary, or other non-public information concerning the Debtors or the Committee, including (without limitation) with respect to the acts, conduct, assets, liabilities and financial condition of the Debtors, the operation of the Debtors' business and the desirability of the continuance of such business, or any other matter relevant to these cases or to the formulation of one or more chapter 11 plans (including any and all confidential, proprietary, or other nonpublic materials of the Committee) whether provided (voluntarily or involuntarily) by or on behalf of the Debtors or by any third party or prepared by or for the Committee (collectively, the "Confidential Information") or (ii) any other information if the effect of such disclosure would constitute a general waiver of the attorney-client, work-product, or other applicable privilege possessed by the Committee.;[76]

- Establishment of a protocol for submission of and responding to creditor information requests;[77] and

- Restrictions on the release of confidential information of third-parties, requiring the committee to first serve notice of the proposed disclosure of such information on counsel for the third-parties whose information was the subject of the request.[78]

The Bankruptcy Court's opinion and order in the *Refco* case mirrors many of the suggestions made by some commentators, who have proposed additional actions to protect confidential and privileged information, including the following:

[74] 336 B.R. 187 (Bankr. S.D.N.Y. 2006).
[75] *Id.*, 336 B.R. at 200.
[76] *Id.*, 336 B.R. at 200-01.
[77] *Id.*, 336 B.R. at 201-02.
[78] *Id.*, 336 B.R. at 202.

- The court can require communications between a debtor and the committee to be on a "for counsel eyes only" basis, in order to invoke attorney-client privilege and work product doctrine;

- The committee can claim negotiations with the debtor are settlement negotiations, and therefore confidential under Federal Rule of Evidence 408;

- The committee can form a subcommittee to handle all communications with the debtor, and then claim that the provisions of the BAPCPA do not cover the subcommittee of a committee;

- The committee can enter into a confidentiality agreement with the debtor, and attempt to rely on this; and

- The committee can seek a court order clarifying procedures to protect confidential information.[79]

C. Practical Considerations in Applying Section 1102(b)(3)

Because Section 1102(b)(3) does not explicitly mention confidential third-party information and does not define the "information" that must be shared by a committee, and because it is likely that creditors who are not members of the committee will push to obtain as much information as possible, the proper scope of Section 1102(b)(3) and the limitations on disclosure that may be imposed by the bankruptcy courts will be an issue in many post-BAPCPA Chapter 11 bankruptcy cases. In-house counsel for companies that possess third-party confidential information and which are considering filing for bankruptcy protection will need to be diligent in alerting bankruptcy counsel to the existence of such information, and to the need to protect it from untoward dissemination and disclosure to committees and to creditors who will seek such information from committees once they are organized. Similarly, in-house counsel for companies that have shared confidential information with businesses that file for bankruptcy will have to take affirmative steps to prevent or limit the disclosure of such information. Such affirmative action should include, at a minimum, negotiating with committee counsel and the debtor over restrictions on the disclosure of confidential third-party information, and insisting upon judicial approval of such restrictions.

Although every case may not justify the level of detail imposed by the Bankruptcy Court in the *Refco* case, each case will require counsel for the committee, counsel for the debtor and third-parties, and the court to evaluate the risk of disclosing confidential third-party information, and the legal and practical limitations that may be

[79] John W. Mills, Colin M. Bernardino, & Daniel A. Fliman, *Committee Confidentiality? New act raises issues by requiring creditor committees to disclose data to noncommittee members,* Nat'l L.J. (November 21, 2005). Other commentators have suggested that the *Refco* decision will serve as a model for courts in other jurisdictions. *See* John J. Rapisardi, Protocol for Creditors' Committee to Provide Information to Constituents, New York Law Journal, May 23, 2006, available at http://www.weil.com/wgm/pages/Controller.jsp?z=r&sz=bl&db=wgm/cbyline.nsf&d=4290A166E9D6A44C8525718000547497&v=0.

imposed on such disclosures. Despite the fact that bankruptcy courts have not spoken with one voice on this issue, the different decisions under Section 1102(b)(3) demonstrate a flexibility and solicitude for safeguarding legitimately confidential information that is encouraging.

FINAL COMMENTS

Bankruptcy, like data security breaches, is a reality of modern American business. Ensuring that the bankruptcy process does not undermine a company's carefully developed data security program will become increasingly important in an era in which the Bankruptcy Code explicitly or implicitly sanctions the sale or disclosure of confidential information notwithstanding such a program. Whether a general counsel represents a company that is considering filing for bankruptcy or is dealing with business partners who are filing for bankruptcy, it is essential that counsel appreciate the privacy protections that Congress has seen fit to interpose into the bankruptcy process. Sensitivity to these provisions will help general counsel steer their clients away from unnecessary data breaches and the attendant negative publicity and potential liability.

Leading the Way in Privacy & Data Security Compliance

John P. Hutchins
Troutman Sanders LLP

In 2005, a rash of high-profile security breaches involving the acquisition of, or access to, large volumes of personal consumer information sparked increased consumer fears of identity theft. In response, many state legislatures have passed statutory schemes requiring consumer notification when such breaches occur. The rationale behind these laws is that early notification will allow affected consumers to take the appropriate steps to prevent or resolve identity theft. To date, some 34 states as well as the city of New York have passed security breach notification laws. At the time of this writing, many other states are still considering legislation.

California pioneered data breach notification to consumers when it passed the California Security Breach Information Act (Senate Bill 1386), which became effective on July 1, 2003. Other states have largely followed the California model, but the statutory details differ from state-to-state. The result is a patchwork regulatory framework that requires careful attention to each potentially applicable state statute. A large-scale breach may affect consumers in many different states. A legally acceptable response as to the affected residents of one state may not be acceptable as to the residents of a neighboring state. As a consequence, the effort needed to develop a multi-state compliance strategy could be significant.

The compliance difficulties presented by these various state laws have prompted Congress to get involved. As many as 34 different data breach notification bills have been introduced during the 2005-2006 term. Most of these bills would, if ultimately passed, preempt state law to one degree or another, but there are competing pressures to avoid weakening some of the more strict state statutory schemes by passing broad, yet relatively weak, federal legislation. At the time of this writing, federal legislation in 2006 appears a remote possibility. Thus, businesses, agencies and other entities covered by the various state laws must be aware of, and do all they can to comply with, the requirements imposed by the various states.

I. Common Elements of Data and Security Breach Notification Laws

While there are many key differences among the various state laws, the general elements of most laws are very similar. The laws generally require that any business which possesses personal information about individual residents of the state enacting the law must disclose a "breach of the security" of such information to all such residents affected by the breach. The schemes employed by most every state, following the model of California SB 1386, address each of the following major issues:

- **What entities are covered?** The statutes define the various entities covered. Most statutes will cover people, businesses, and state agencies. Most states restrict the scope of coverage in some manner, usually by applying only to entities with personal information collected on a certain baseline number of individuals, such as 5,000 or 10,000. Some states further restrict the scope of their scheme by analyzing the purpose for which the information is collected. For example, Georgia's statute applies only to

"information brokers," defined as entities that collect data for the purpose of selling the data to third parties for a fee. Other states provide exemptions for certain entities already governed by other statutes, rules, and regulations regarding data security, such as the Gramm-Leach-Bliley Act.

- **What type of information is covered?** Generally, the statutes apply to sensitive, unencrypted "personal information." This is usually defined as a person's first name or first initial and last name used or stored in combination with any one or more of the following: social security number, driver's license or non-driver's identification number, credit or debit card or other financial account number in combination with any required access code. However, various states define "personal information" or "personally identifiable information" in different ways. For instance, Georgia defines protected information to include a last name and a PIN number, even though it is difficult to imagine how a person's personal identify could be compromised if a third party has access to a name and a PIN, without more information like a credit card number to which that PIN relates. Moreover, some statutes apply only when there is a breach of any unencrypted "personal information" – however the particular statute defines it. But other statutes apply even when a portion of the identifying information is encrypted. Like the example from Georgia, it is unclear what harm could come to a person when encrypted information is compromised, simply because a piece of unencrypted information is also compromised. Without at least two items of unencrypted information, it is difficult to imagine how a potential identity thief could use the information.

- **What constitutes a breach?** Under the various states' laws, there are differing treatments of whether notice is required following the unauthorized acquisition of, or merely unauthorized access to, computerized data. Generally speaking, however, the touchstone is the possibility that the security, confidentiality or integrity of personal information has been compromised. Notice requirements are usually triggered if personal information was in fact accessed or acquired **or** if personal information is "reasonably believed" to have been accessed or acquired. A few states actually require some probability of harm (i.e., notice is not required unless there is a reasonable basis or belief that the breach will result in substantial harm to the affected persons). But this is not the majority approach.

- **Who must be notified?** Notice must be given to all residents of the enacting state whose unencrypted personal information was the subject of the breach. It is the residency of the affected persons, not the location of the breach, that controls. Often, therefore, the laws of multiple states are implicated by one breach. If, for example, a breach occurs in Florida, but personal information for residents of all 50 states is involved, notification must be given in compliance with each state that has adopted a breach notification statute.

- **How quickly must notice be provided?** Most of the statutes require notice to be given to affected residents in the most expedient time possible and without unreasonable delay. Generally, delay is allowed to comply with the legitimate needs of law enforcement or to determine the scope of the breach and restore the integrity of the data system.

- **What is the form or method of notification?** Most state laws are quite vague about what constitutes valid notice. Most states contemplate some sort of written notice. Some states allow for electronic notice under limited circumstances, usually if such notice is consistent with the federal Electronic Signatures in Global and National Commerce Act ("E-SIGN"), 15 U.S.C. § 7001 *et seq*. Practically speaking, however, electronic notice of a data breach would be rare under E-SIGN, unless the subject of the data breach to be notified had previously consented to electronic notice. Some states also allow for telephone notice. Substitute notice is allowed if the cost of providing notice with one of the above methods is too expensive (usually more than $250,000) or if more than a certain number of people are affected (usually 500,000 or more). If substitute notice is a viable option, it must usually consist of all of the following: (1) electronic mail (e-mail) notice when there is an e-mail address for the affected people; (2) conspicuous posting of the notice on the website of the covered entity; and (3) notification to major statewide media.

- **How do the notification requirements differ for those who simply "maintain" personal information?** Some states treat those who merely maintain information different from those who own, license or lease it. In general, requirements for "maintainers" in these states differ in two respects. First, those who maintain personal information do not have to provide any manner of notification to the affected individuals; that notification is the responsibility of the owners, licensees or lessees. Those who maintain personal information must simply notify the owners, licensees or lessees. Second, this notification must be provided immediately.

- **Is there a safe harbor for those companies that already have notification procedures in place?** In a majority of the states, entities may be deemed compliant if they maintain and comply with their own notification procedures as part of an information security policy for the treatment of personal information, to the extent such procedures are consistent with the breach notification statute itself.

- **Must notification be given to any additional parties?** In many states, in addition to notifying affected residents, covered entities must also notify other parties such as consumer reporting agencies or the state attorney general's office.

- **How is the statute enforced and what are the potential penalties?** All but a few of the state statutes include an enforcement provision, but rules are generally vague. Typically, the state attorney general is responsible for enforcement. Some state statutes set forth the potential penalties in the text itself, while other states simply reference a separate state code section. Penalties vary widely by state.

II. The Difficulty of a Multi-State Strategy

While most states follow some version of the California model, many significant and key differences appear throughout the landscape of these data security statutes. In some cases, a seemingly small difference in language from one state to another can have a large impact on

what is considered an appropriate response. The following sections outline the major differences and their potential impact.

The Triggering Event

The single biggest difference among the various state statutes is whether a triggering event is included. In many of the states, including California, the notification requirements are triggered whenever there has been an event that causes the covered entity to reasonably believe there has been unauthorized access to or acquisition of computerized data that compromises the security, confidentiality or integrity of personal information. In other states, however, simple access or acquisition is not enough to trigger the notification requirements. In these states, notification is only required if there is a reasonable likelihood of harm to the affected individuals or if the breach is material. Thus, there is no "automatic" trigger but, rather, a subjective standard to be applied.

The Entities Covered

A typical statute applies to all state agencies, as well as people and businesses that conduct business in a particular state. However, many state statutes do not apply to state agencies. Further, not every statute uses such generic terms. Georgia uses the term "information brokers." Illinois and Nevada use the term "data collectors." Tennessee uses the term "information holder." It is important, therefore, to pay attention to who is covered under the statute and how the statute defines the covered entities.

The Information Covered

As mentioned above, the typical statute covers "personal information," which is generally defined as a person's first name or first initial and last name in combination with any one or more of the following: social security number, driver's license or non-driver's identification number, credit or debit card or other financial account number in combination with any required access code. Many states have broadened this definition, however. Maine, for example, does not require an individual's first or last name to be included if the other information alone is enough for an unauthorized person to fraudulently assume or attempt to assume the identity of an individual. Once again, one must be certain of such a distinction because it directly affects whether notice must be provided to the residents of a particular state.

Penalties and Enforcement

Perhaps more than any other aspect of these state statutes, the penalties and enforcement methods vary most from state-to-state. Many of the states provide for attorney general enforcement. Others, such as California, provide a private right of action. And in states such as Arkansas, it is unclear. Section 4-110-108 of the Arkansas Code states that any violation is punishable by action of the Attorney General, but then goes on to incorporate by reference sections 4-88-101 through 4-88-115. Section 4-88-113(f) specifically provides for private rights of action. One could argue, therefore, that although the Attorney General is given enforcement powers under the statute, the incorporation of section 4-88-113(f) preserves the right of an injured individual to bring suit.

The potential remedies and penalties vary widely. Many states allow for injunctive relief to prevent covered entities from continuing to violate the statute's requirements. Some states, such as Arkansas and Connecticut, allow for the dissolution, suspension or forfeiture of corporate charters or the right to conduct business in the state. Many other states provide for varying levels of fines and civil penalties.

III. Ounce of Prevention Worth A Pound of Cure

One would think that, with all of the activity surrounding passage of dozens of data breach notification laws, such laws would be working to reduce the number of breaches. However, in 2006 alone, there have been nearly 100 separate incidents from which an organization reported the compromise of personally sensitive information on individuals, affecting more than 6 million people. And some of these breaches are not even covered by the new patchwork of state laws. In early August 2006, AOL apologized for accidentally posting on the Internet about 19 million search requests made by about 658,000 subscribers during a three-month period ending in May. The data was gathered for "research purposes," according to AOL. Because none of the exposed data contained "personally identifiable information," as defined by the data breach notification statutes, however, it does not implicate any of these statutes.

Thus, although CIO.com Assistant Editor Sarah Lourie once wrote that SB 1386 "uses fear and shame to make companies think more seriously about information security," it does not appear to be actually changing the behavior of many companies with mountains of sensitive data meriting protection – even the most technology-savvy companies. Public and private companies, federal and state government agencies, non-profits, educational institutions and many other types of entities have experienced security breaches for which notice has been required. They come in all shapes and sizes. Some are the result of a business being defrauded into turning over information willingly. Some are the result of a sophisticated computer "hack." Some are the result of simple larceny. Some are the result of basic human error, like losing a laptop. Some are the result of a third-party's non-performance, like an electronic storage vendor who loses data in transit. And data breach notification laws, unlike other privacy laws such as FCRA, HIPAA or Gramm-Leach-Bliley, generally do not include requirements regarding restrict access to or use of consumers' personal data. They simply empower consumers to manage their own personal information, and, using "fear and shame" attempt to motivate data owners to step up security. But the sheer variety of breaches should be leading people to evaluate what data they have and what they should be doing to manage it.

Federal legislation has stalled, but the Federal Trade Commission is not waiting for legislation. It is aggressively policing the information security practices of American businesses. Within the past 18 months, the FTC has brought and settled at least four high-profile actions with companies that suffered security breaches. The source of the agency's authority is not clear. Nonetheless, it purports to rely on the Federal Trade Commission Act, which prohibits "unfair" and "deceptive" trade practices. The FTC has counted on "fear and shame" to motivate companies targeted by these "privacy initiatives" to settle. Its allegations in the actions it has

brought have been fairly consistent. It has generally alleged that the company that is the target of its action:

- Failed to encrypt consumer data when it was stored or transmitted
- Created unnecessary risks to information in the way that it was stored
- Failed to use readily available security measures to prevent unauthorized access or false authentication
- Failed to use sufficient measures to detect unauthorized access or to conduct appropriate security investigations

Despite its nebulous authority to act in these data breach matters, the FTC has been able to reach settlements with all of the targets of its actions, and all of the settlements have involved substantial fines and payments. Through these "privacy initiatives," the FTC has also imposed extensive requirements regarding data security programs. In doing so, the agency is creating its own, de facto, regulatory scheme.

The assistant director of the FTC's newly formed Division of Privacy and Identity Protection, Betsy Broder, was quoted in the March 2006 issue of *ABA Journal* as saying, "Unless you're one of a few businesses that are exempt from our jurisdiction, like insurance companies, we will act against businesses that fail to protect their customer data." Broder said that all business should look to Gramm-Leach-Bliley, which specifically applies only to "financial institutions" for guidance on how to protect consumer data. According to Broder, "At a basic level . . . businesses need to have a plan in writing describing how customer data is to be secured and an officer on staff responsible for implementing that plan." *ABA Journal*, March 2006, p. 40.

What Broder means when she refers to "guidance" from Gramm-Leach-Bliley is actually something called the "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice." These guidelines were issued in March 2005 by Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency and the Office of Thrift Supervision. In essence, these guidelines establish the "gold standard" regarding best practices in developing an information security program. The guidelines establish the following phased approach to implementing such a program:

First, the organization should conduct a risk assessment and identify the following:

- Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems
- The likelihood and potential damage of threats, taking into consideration the sensitivity of customer information
- The sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks[1]

[1] Under the guidelines, "customer information systems" consist of all of the methods used to access, collect, store, use, transmit, protect, or dispose of customer information including the systems maintained by its service providers.

Following this assessment, the guidelines require a program designed to address the identified risks. The particular security measures an organization should adopt will depend upon the risks presented by the complexity and scope of its business. At a minimum, the guidelines require an organization to consider the specific security measures enumerated in the guidelines, and adopt those that are appropriate for the institution, including:

- Access controls on customer information, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means
- Background checks for employees having access to customer information
- Response programs that specify actions to be taken when the organization suspects or detects that unauthorized persons have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies

The guidelines also direct that service providers be required by contract to implement appropriate measures designed to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. In addition to such contractual obligations, a service provider may be required to implement a comprehensive information security program of its own.

IV. When the Dike Breaks: Responding to the Inevitable Data Breach

The guidelines also require a program in place to response to a data breach, if it occurs. At a minimum, an organization's response program should contain procedures for the following:

- Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused
- Notifying primary regulators as soon as possible when the organization becomes aware of an incident involving unauthorized access to or use of sensitive customer information
- Notifying appropriate law enforcement authorities
- Taking appropriate steps to contain and control the incident to prevent further unauthorized access, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence
- Notifying customers when warranted[2]

In addition to recognizing that the guidelines exist and that the FTC is relying heavily on the guidelines in enforcement actions, the long list of data breaches in 2005 and 2006 should provide in-house counsel with a simple takeaway: No one is immune. "Experience makes it apparent that attempts to prevent data loss will ultimately fail," wrote Drew Robb in the September 19, 2005 issue of *Computerworld*. The issue is not *whether* a business will experience

[2] Where an incident of unauthorized access involves customer information systems maintained by an organization's service providers, it is the responsibility of the organization whose vendor experiences the breach to notify that organization's customers and regulators.

a data breach triggering statutory disclosure obligations and subjecting it to public shame. Rather, the issue is *how* that business will respond when the inevitable happens. A statutorily-mandated breach disclosure will, for most companies, create a near-term public relations crisis. Fortunately for those who were not among the first to disclose data breaches under SB-1386, the experiences of those who were have created a template for how to respond. There are several key points to remember.

First, companies can take preventative action. Many companies within the last few years have created a chief privacy officer or similar position, even when data collection is not their core business. All substantial businesses should consider creating such a position, or at least tapping an existing corporate officer with the duties of such a position and including this position in her title. The very act of creating the position evidences heightened concern for data security and privacy. It also serves two practical ends. It sends a clear message to customers, as well as potential data thieves, that the company's eye is on the data-security ball. If it is the job of no one in particular to keep an eye on that ball, it is more likely to hit the ground at some point. Having someone in charge who focuses on privacy and data security will certainly help avoid some problems that might otherwise arise. Also, ordaining a chief privacy officer may help address post-breach claims that a company cavalierly ignored the importance of privacy and data security. As with many other issues that create potential liability, it is important to have policies in place and the ability to point to tangible actions taken to help minimize harm. The very existence of a chief privacy officer who manages policies aimed at preventing a breach may provide good defenses to claims asserted in the aftermath of a breach, either by the media or by lawyers.

Second, corporate America should be aware that, even though a company experiencing data loss may be a crime victim, the public will not view it that way. The public views the individuals whose data was lost or stolen as the victims, even though they may not have experienced actual harm. Plaintiffs' lawyers are claiming harm from "the anxiety of waiting and wondering." Although it remains to be seen what judges will do, it is possible that the public (which makes up juries) might ignore established damages principles and accept that theory. Businesses should keep this in mind when considering a public response.

Third, senior management needs to be immediately available to the media and they should tell the media what they know as soon as possible. They should also move to assure that:

1. personnel and systems aimed at preventing data breaches are in place;
2. an investigation is undertaken regarding the cause of the breach;
3. the situation that led to the breach is being or has been remedied; and,
4. a top-down review of personnel and systems is underway in order to *attempt* to prevent future breaches.

Management should quickly communicate these assurances to the public, at the very least, and consider going even further. For instance, ChoicePoint over-notified by a wide margin, issuing nationwide notices (not just to Californians) and also offering assistance to consumers whose information may have been compromised. This sort of extra effort will go a long way toward muting the public outcry. Perhaps most important, without admitting any liability, the company should publicly apologize for any inconvenience the data breach might cause the people whose data was lost or stolen.

Finally, when a business experiences a major data breach, it should be prepared to defend a variety of claims asserted in various class action lawsuits. The deeper the company's pockets, the greater the likelihood of a lawsuit. It will likely take years to sort out the legalities of such claims. Until that happens, plaintiffs' lawyers will continue to test a number of different theories. It appears that the plaintiffs' bar already hopes this is the next asbestos or tobacco bonanza.

Disaster Preparedness

Companies that developed a "crisis preparedness plan" in the wake of 9/11 should consider including data breaches as part of that plan. Basic crisis preparedness planning includes aspects particularly important to data breach responses:

1. identifying who will be in charge; and,
2. identifying specifically which persons are responsible for communicating with various constituencies (i.e., employees, customers, government, media, etc.).

Such a plan might also anticipate other important issues. Who should be contacted in addition to those required by disclosure statutes? Are there friendly media contacts identified in advance? What regulators should be notified and how? This is not just a plan for PR spin. It should set forth precisely what the company intends to do in the event of a data breach. The spate of data breaches in 2005-2006 shows that companies that respond quickly fare far better.

Privacy concerns are at an all-time high. Government is imposing new and significant regulation. The way companies store and use personal data is now a matter of national policy debate. Depending on the business, a data breach can bring a company to its knees. At the very least, it can expose a company to significant potential liability. Senior management needs to recognize the risk and anticipate a response. Waiting until a breach occurs will leave a company flat-footed, and the public response will be costly.

Practical Considerations of Notice

Finally, there are some practical considerations to take into account when notifying customers of a data breach:

First, there is the issue of the notice itself. Most state data breach laws say virtually nothing about the content of the notice, except in very vague terms. Even the federal guidelines governing Gramm-Leach-Bliley provide very little meaningful guidance (or restrictions) regarding content notice. The guidelines only require that notice be given in a clear and conspicuous manner, that it describe the data breach incident in general terms and the type of data that was the subject of unauthorized access or use and that it generally describe what the organization has done to protect the customers' information from further unauthorized access. The guidelines also provide that the notice should include a telephone number that customers can call for further information and assistance and that it remind customers of the need to remain

vigilant over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft.

The guidelines also suggest that the notice include the following additional items, when appropriate:

- A recommendation that the customer review account statements and immediately report any suspicious activity;
- A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports to put the customer's creditors on notice that the customer may be a victim of fraud;
- A recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;
- An explanation of how the customer may obtain a credit report free of charge; and,
- Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft, including encouragement that the customer report any incidents of identity theft to the FTC, and a toll-free telephone number that customers may use to obtain the FTC's identity theft guidance and report suspected incidents of identity theft.

Nothing in the guidelines, however, precludes the use of the notice for the purposes of old-fashioned public relations or marketing. Those providing notice should consider using the communication to enhance customer confidence. In September 2005, *ComputerWorld* reported the results of a Ponemon Institute survey of more than 1,000 people who had received notice of personal data security breaches. Twenty percent said they had already terminated their relationships with the companies that maintained their data. Another 40% said they might do so, and nearly 5% said they had hired lawyers to seek legal recourse after their data was put at risk. Given these high stakes, it would border on foolish for any company sending a data breach notice not to use the opportunity to communicate with its customers in as positive a manner as possible about the companies business, services, products or brand in an effort to restore whatever measure of goodwill may have been lost from the fact of the breach notice.

Notifying Consumer Reporting Agencies

The guidelines encourage, and many state laws require, that organizations reporting a breach also notify the nationwide consumer reporting agencies of the breach. This is a peculiar requirement, indeed, because CRAs are not in the business of doing anything other than reporting on a credit report information provided to them by creditors, either positive or negative, about a particular consumer's payment history and credit worthiness. Thus, the mere fact that a consumer's data has been or may have been compromised is not information that CRAs are in a position to use for the benefit of consumers, creditors or any other element of a CRAs constituency. Perhaps the reasoning behind the requirements of CRA notification is the idea that, once receiving notice, masses of people will contact CRAs to review their credit file and will dispute negative information that they perceiving as arising from the breach, and the legislators drafting data breach notification statutes desired to make sure that CRAs are not caught flat-footed by an unexpected rash of inquiries by consumers. The CRAs themselves, however, seem to be unconcerned about this eventuality.

As of the date of this writing, none of the three major credit bureaus have any formal process in place for receiving data breach notifications from the companies who are required to send them to consumers. In fact, most of the statutes that require CRA notification say very little about what one must do to comply with this requirement. Typically, the statute's only direction is that the CRAs be notified of the timing, distribution, and content of the notices. In most states, compliance is likely achieved by a simple letter, addressed to the registered agent of a CRA, which says, for example, "On September 1, 2006, ABC Company notified 6000 consumers of a potential data breach, as more specifically described in the attached notice, which is a sample of the letter that was mailed to affected consumers."

Delivery of Customer Notice

Other than perhaps some basic guidance regarding the content of the notice, most data breach notification statutes do not define what constitutes sufficient written notice. For example, the statutes give no guidance as to whether "last known address" is sufficient, whether bulk mail is acceptable, or what to do if a notice is returned for insufficient address. If notices must be sent to a very large number of consumers, the mailing costs could be substantial. First class mail is not typically required by statute, however, and bulk mail should be considered.

Typically, all large scale notification mailings (whether first class mail or bulk mail) will garner a certain number of notices that are returned for one reason or another, likely because consumers have moved or their contact information was incorrectly given, received or stored well before the breach notification occurred. What a company should do upon receiving returned notices is not delineated in any statute. Generally, companies should consider checking the returned notices to assure that whatever address is included on each notice is the best, last known address on file with the company and then resend the notices in the same manner as they were sent the first time. If notices are returned a second time, the company can certainly argue that its notice attempts to these particular consumers was reasonable under the circumstances.

Conclusion

Information is a key commodity in the 21st century. Yet, most companies do not have good information management policies. An estimated 70% of companies today do not even have Internet use policies, much less comprehensive information management policies. Even companies with good policies lack effective implementation, training or enforcement. Few companies treat information like the key commodity that it is in today's business environment. Companies that do are well ahead of their competitors.

Most companies of any significant size should consider implementing a comprehensive Information Management and Protection Program. Federal legislation may soon require such a program for companies with as few as 1000 customers, and the Federal Trade Commission is already exercising regulatory authority in the arena, even though the source of that authority is

not clear. Companies that implement a comprehensive program, including a crisis management component to deal with the inevitable data breach, will reduce the chances of a large-scale loss of critical data that could lead to bad press, exposure to legal liability or massive customer defections.

Data Collection: Everyone's Doing It

- Electronic Commerce Has Led to Explosion of Data
  - Between 2002-2005, the world will generate more data than all the data generated on earth over the last 40,000 years.

University of California at Berkeley Study

The Evolution of Privacy Law

- 1970 – Nation's First Privacy Law
  - Fair Credit Reporting Act (FCRA)
- Intended to regulate the growing credit reporting industry, which compiled "consumer credit reports" and "investigative consumer reports" on individuals
- FCRA was the first federal law to regulate the use of personal information by private businesses
- Purpose is to promote accuracy, fairness, and privacy of personal information compiled by CRAs

The Evolution of Privacy Law

- 1996 – HIPAA
- Health Insurance Portability and Accountability Act
- Allows portability for group coverage from one carrier to another group carrier; limits imposition of "pre-existing condition"

ACC 2006 Annual Meeting: The Road to Effective Leadership

The Evolution of Privacy Law

- Rules promulgated specifying series of safeguards (administrative, technical, physical and organizational) to assure availability, confidentiality, and integrity of electronic health information
- ***Standards for Privacy of Individually Identifiable Health Information,*** also known as the "HIPAA Privacy Rule"
- Establishes, for the first time, a set of national standards for the protection of certain health information
- Goal to assure that individuals' health information is properly protected while allowing flow of health information to provide and promote quality health care

The Evolution of Privacy Law

- 1999 – Gramm-Leach-Bliley Act
- Repealed the 66-year old Glass-Steagall Act, which prohibited banks, securities firms and insurance companies from affiliating
- Permits financial institutions to share personal customer information with certain affiliates
- Requires financial institutions to disclose policies and practices regarding sharing of non-public personal information
- Allows customers to opt-out of information sharing arrangements to non-affiliated third-parties

ACC 2006 Annual Meeting: The Road to Effective Leadership

California SB 1386

California Information Practice Act or Security Breach Information Act

- First in the nation, effective July 1, 2003
- 2005 – "The Year of the Data Breach"
- Approximately 150 separate incidents in which an organization reported the compromise of personally identifiable information on individuals
- Affecting approximately 57 million people
- Dozens of breach notification laws passed
  - 23 states and New York City

California SB 1386

- "Law uses fear and shame to make companies think more seriously about information security"
- First reports in 2005 opened media floodgates
- Copycat legislation, lawsuits, new legal theories, technical reactions (encryption)

The Evolution of Privacy Law

- 2006 – The Laws Are Working, Right?
- Approximately 181 separate incidents in which an organization reported the compromise of personally identifiable information on individuals (*www.privacyrights.org*)
- Affecting approximately 34 million people
- Laws still being passed, and 10 federal bills pending

Common Elements of Data Breach Notification Laws

- What entities are covered?
- For what purpose is the information collected?
- What type of information is covered?
- What constitutes a breach?
- Who must be notified?
- How quickly must notice be provided?

Common Elements of Data Breach Notification Laws

- What is the form or method of notification?
- How do the notification requirements differ for those who simply "maintain" personal information?
- Is there a safe harbor for those companies that already have notification procedures in place?
- Must additional parties be notified?
- How is the statute enforced and what are the potential penalties?
- What is the triggering event requiring notification?

What Entities Are Covered?

- People, state government agencies, for-profit and non-profit organizations
  - Some restricted by the number of records
- All "data collectors" who maintain computerized "personal information"
  - Few look at purpose for which data maintained

What Conduct is Covered?

- Requires that any business that *owns or licenses* computerized data that includes *personal information* to give *notice* of any *breach of the security of the data* following discovery of such breach to any resident of the state whose unencrypted personal information was or is reasonably believed to have been accessed and/or acquired by an unauthorized person

Personal Information ("PII")

- Person's name in combination with:
  - social security number
  - driver's license or non-driver's identification number
  - credit or debit card or other financial account number in combination with any required access code

NOT Personal Information

- Personal Information specifically does not include "information lawfully made available to the general public from federal, state or local government records"

Breach of the Security of the "System"

- Unauthorized *acquisition* of an individual's computerized data that compromises the security, confidentiality, or integrity of personal information of such individual
- Does not include "good faith" acquisition, as long as no "bad faith" use or "subject to further unauthorized disclosure"
- NOTE: Not necessarily limited to a breach of a computer system, despite the word "system" in the definition

ACC 2006 Annual Meeting: The Road to Effective Leadership

Notice

- Written notice (addressed to whom?)
- Electronic notice, if provided consistent with provisions federal Electronic Signatures Act (basically, consumer consents)
- Substitute notice

"Do-It-Yourself" Notice

- If
  - Person or business that has its own notification procedures, as part of an information security policy for the treatment of personal information; and,
  - Policy is consistent with timing requirements of governing statute
- Then
  - Compliance with policy = compliance with statute

Time Requirements

- "Most expedient time possible and without unreasonable delay"
- Potentially long delay for
  - legitimate needs of law enforcement
  - any measures necessary to determine scope of breach and restore the data system's reasonable integrity

Notice to Additional Parties

- Consumer Reporting Agencies
- States' Attorneys General
- Secret Service

Remedies

- Civil suit for damages
  - Private Right of Action
  - Action to State Attorney General
- Injunction
- Actions for data breach itself
  - Class Actions
  - Enforcement by Federal Trade Commission, States' Attorneys General, Regulatory Agencies

The Evolution of Privacy Law

- **Fundamental Shift**
  - Notification
  - Liability/Enforcement
  - Standards

ACC 2006 Annual Meeting: The Road to Effective Leadership

Where Are We Headed?

- **Information Management and Protection Programs**
  - Standards for developing and implementing administrative, technical, physical and organizational safeguards to protect the security of sensitive personal information
  - Regular assessment, management and control of risks to data privacy and security
  - Publish Information Security policies
  - Employee training
  - System tests
  - Vendor compliance

Information Management and Protection Programs

- Proposed federal legislation
  - One year to comply
  - Significant fines for non-compliance
- Violations
  - "civil penalties" of $5,000 per day, up to $35,000 per day
  - double penalties for willful violation

FTC "Privacy Initiatives"

- The Federal Trade Commission not waiting for legislation
- Aggressively policing the information security practices of American businesses
- Within the past 18 months, the FTC has brought and settled four high-profile actions with companies that suffered security breaches
- Source of authority not clear
  - Purportedly the Federal Trade Commission Act, which prohibits "unfair" and "deceptive" trade practices
  - Until now, "unfair" and "deceptive" have been interpreted as nearly synonymous terms
- All of the settlements involve substantial fines and require extensive data security programs

FTC Regulation

- Counting on "fear and shame" to motivate companies targeted by "privacy initiatives" to settle
- Creating its own precedent?
- Creating standards for data security programs
- Federal regulation is here, regardless of whether federal legislation passes or not

ACC 2006 Annual Meeting: The Road to Effective Leadership

FTC Regulation

- Newly formed Division of Privacy and Identity Protection
  - Betsy Broder, Assistant Director
    - "Unless you're one of a few businesses that are exempt from our jurisdiction, like insurance companies, we will act against businesses that fail to protect their customer data."
    - All business should look to Gramm-Leach-Bliley, which specifically applies only to "financial institutions," for guidance on how to protect consumer data.
    - "At a basic level . . . businesses need to have a plan in writing describing how customer data is to be secured and an officer on staff responsible for implementing that plan."

ABA Journal, March 2006, p. 40

Toward a Data Security Standards

- Broder reference to "guidance from Gramm-Leach-Bliley"
  - "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice"
  - Issued in March 2005 by Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency and the Office of Thrift Supervision
  - Establishes "gold standard" regarding best practices in developing an information security program

Toward a Data Security Standard

- Phase I
  - Risk assessment to identify:
    - Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of PII or PII systems
    - Likelihood and potential damage of threats, taking into consideration the sensitivity of PII
    - The sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks

Toward a Data Security Standard

- Phase II
  - Risk-based program, including (minimum):
    - Access controls on PII, including controls to authenticate authorized individuals and prevent employees from providing PII to unauthorized individuals who seek to obtain information fraudulently
    - Background checks for employees having access to PII
    - Response programs specifying actions to be taken when unauthorized access is suspected, including appropriate reports to regulatory and law enforcement agencies
    - Requirement that service providers be required by contract to implement appropriate measures designed to protect against unauthorized access to or use of PII
      - Services providers may be required to implement a comprehensive information security programs

ACC 2006 Annual Meeting: The Road to Effective Leadership

A Case Study: Toward a Data Security Standard – The Payment Card Industry

Credit Card Security in Retail

- Background
  - FCRA – credit reporting industry
  - GLB – financial services industry
  - HIPAA – healthcare industry
  - Credit card fraud losses on upward trend

PCI – Data Security Standard

- 2001: Visa®U.S.A. mandated CISP – Cardholder Information Security Program
  - 2004: Aligned with MasterCard International® SDP – Site Data Protection and renamed
  - 2006: American Express®, Discover®Card, Diners Club®, JCB® signed onto the program

Perspective of a security professional

- Is the risk of a breach eliminated? No
- Are the requirements excessive? No
  - Controls are basic and uncontroversial
  - Consistent with ISO and US NIST
- Are the requirements clear? Yes
- Decisions needed to select controls? No
- Is it a total security program? No

FTC Act, Section 4

- Inadequate security as a trade practice
  - BJ's Wholesale Club, Inc. File No. 0423160
    - Did not encrypt credit card data
    - Lack of access control on stored data
    - Lack of security controls on wireless infrastructure
    - Lack of detective controls or investigative measures
    - Excessive retention of data

Decision on BJ's

- Third party audits mandated for 20 years
- Definitions of personal information expanded further from GLB
- Comprehensive security program required
  - Designation of accountable employee(s)
  - Risk assessment required
  - Risk controls required
  - Ongoing adjustments to security program

ACC 2006 Annual Meeting: The Road to Effective Leadership

BJ's SEC Filing, as of April 29, 2006

- A leading security firm conducted forensic analysis and reached these conclusions:
  - No conclusive evidence of a breach
  - Centralized systems had not been breached
  - Any possible breach would be at store level
- As of May 31, 2006, $13 million in outstanding claims
- Unable to predict any further claims

PCI DSS applied to BJ's

- Credit card data encrypted
  - PCI DSS Sections 3.4, 3.5., 3.6 and 4
- Access control on stored data
  - PCI DSS Sections 7, 8, 9
- Security control on wireless infrastructure
  - PCI DSS Section 2
- Detective controls or investigative measures
  - PCI DSS Section 11
- Minimum retention of data
  - PCI DSS Section 3.1

DSW, Inc., FTC File 052 3096

- March, 2005, inadequate security complaint
  - Stored data in multiple files without need
  - Did not use available security measures
  - Lacked encryption on stored data
  - Inadequate access controls
  - Insufficient network controls
  - Failed to employ detective measures

FTC Decision on DSW, Inc.

- Expanded definitions of “personal information” beyond GLB
- Visa submitted public comments
- Bank of America offered public comment

PCI DSS applied to DSW, Inc.

- PCI DSS audit documentation would have addressed every point on the complaint
- PCI DSS would have significantly mitigated the risk of a breach

Favorable features of PCI DSS

- No decisions → No expensive consultants on selecting appropriate controls
- Can be updated for new or changing threats or as new technologies are developed
- Audit schedules relate to volume of data
  - Small merchants can self-assess
  - Large merchants must use third parties
  - Volume determines frequency

Quote from Visa: Why comply?

- Everyone benefits
  - Limits risk
  - More confidence in payment industry
- Merchants & Service Providers
  - Competitive edge
  - Increased revenues and improved bottom line
- Consumers
  - Information is safeguarded
  - Identity theft protection

Toward a Data Security Standard

Incident Response Plan

- Comprehensive Incident Response Plan
  - Data Breach
  - Disaster Recovery
  - Infringement or Misappropriation
- Crisis Management Committee
  - Who's got the ball?
  - In what circumstances?
  - "I'm in control here."

Incident Response Plan

- Betsy Broder, FTC
  - "At a basic level . . . businesses need to have a plan in writing describing how customer data is to be secured and an officer on staff responsible for implementing that plan."
- All substantial businesses should consider creating CPO level position
  - At least tap existing corporate officer with the duties of such a position and include position in her title
  - Very act of creating the position evidences heightened concern for data security and privacy
    - Sends a clear message to customers, as well as potential data thieves, that the company's eye is on the data-security ball
- If it is the job of no one in particular to keep an eye on the ball, it is more likely to hit the ground at some point.

No One Is Immune! It <u>will</u> happen to you.

- "Privacy breaches" come in all shapes and sizes
  - Some are the result of old-fashioned fraud
  - Some are the result of a sophisticated computer "hack"
  - Some are the result of simple larceny
  - Some are the result of basic human error (i.e., it's just lost)
  - Some are the result of a third-party's non-performance
- Approximately 335 reported breaches in less than two years
  - Federal government agencies; world's biggest financial institutions; "big four" accounting firms, Fortune 100 companies

Incident Response Plan

- Assess nature and scope of incident; identify what PII systems and types of PII have been accessed or misused
- Notify primary regulators as soon as possible when organization becomes aware of an incident involving unauthorized access to or use of PII
  - Notify appropriate law enforcement authorities
  - Taking appropriate steps to contain and control incident to prevent further unauthorized access, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence
  - Notify customers when warranted

Incident Response Plan

- Be aware that, even though a company experiencing data loss may be a crime victim, the public will not view it that way
- Senior management should be immediately available to media; tell the media what you know as soon as possible
- Management should quickly communicate assurances to the public, at the very least, and consider going even further
- Public relations strategy should be in place

ACC 2006 Annual Meeting: The Road to Effective Leadership

Post-Crisis Management

- Preventing future problems by identifying factors that led to the problem creating the crisis
- Two types of future problems
  - Lawsuit
  - Repetition of incident
- Multiple potential post-crisis responses to address each
  - Employee discipline
  - Changes to systems
  - Data deletion or destruction

No. 1 Reason to Implement Information Management and Protection Program?

- September 2005 survey
  - More than 1,000 people who had received notice of personal data security breaches
    - 20% said they had already terminated their relationships with companies that maintained their data
    - Another 40% said they might do so
    - Nearly 5% said they had hired lawyers to seek legal recourse after their data was put at risk

The New Paradigm: Specific Applications of Concern for Privacy – The Bankruptcy Abuse Prevention and Consumer Protection Act of 2005

General Background Regarding BAPCPA

- BAPCPA signed by President Bush on April 20, 2005
- Most comprehensive revision of U.S. Bankruptcy Laws since 1978
- Generally effective as to bankruptcy cases filed on or after October 17, 2005

Four Major Privacy-Related Changes

- Restrictions on sale of PII
- Restrictions on access to and destruction of confidential patient records in health care bankruptcies
- Restrictions on disclosing names of minor children and means of identification
- Unsecured creditors' access to information

Personally Identifiable Information

- New Code §101(41A) defines PII to generally include all personal information about individual consumers held by a debtor
- Encompasses "any . . . information concerning an identified individual that, if disclosed, will result in contacting or identifying such individual physically or electronically."
- Includes names, addresses, e-mail addresses, phone numbers, social security numbers, etc.

Restrictions on Sale of PII

- Section 363(b)(1) restricts sale of PII in possession of debtor *if* the debtor had a policy prohibiting or restricting the transfer of PII which was disclosed to consumers and in effect on the petition date
- **No restriction on sale of PII if debtor had no policy in effect on petition date**

Restrictions on Sale of PII

- PII may only be sold if -
  - Sale consistent with debtor's existing policy, or
  - A consumer privacy ombudsman is appointed and the court approves the sale after notice and a hearing

ACC 2006 Annual Meeting: The Road to Effective Leadership

Consumer Privacy Ombudsman

- New Section 332 regulates appointment of consumer privacy ombudsman ("CPO")
  - Must be appointed at least 5 days before hearing on whether or not PII should be sold
  - Must be "disinterested person" other than U.S. Trustee
  - May be compensated from bankruptcy estate pursuant to amended Section 330(a)

Consumer Privacy Ombudsman

- Interim Bankruptcy Rule 6004(g) requires motion for authority to sell PII to include request for order directing appointment of CPO
- Interim Bankruptcy Rule 2002(c)(1) requires notice of motion for authority to sell or lease PII to state whether proposed sale or lease is consistent with a policy prohibiting transfer

Privacy Issues Related to Health Care Businesses

- "Health care business" defined by new Code § 101(27A) as any public or private entity involved in virtually any way in providing health care to the general public
- Includes hospitals, nursing homes, ambulatory, emergency and urgent care facilities, hospices, and home health agencies

Restrictions on Destruction of Confidential Patient Records

- New Code § 351 requires trustee or debtor-in-possession to destroy confidential patient records of a debtor that is a health care business if it becomes too expensive to maintain the records
- These rules apply in any case under Chapter 7, 9 or 11 of the Bankruptcy Code

Prerequisites to Destruction of Patient Records

- Trustee must publish notice of intent to destroy records 365 days after first publication of notice in "1 or more appropriate newspapers"
- Trustee must also attempt to notify patients and their health insurers directly within first 180 days of the 365 day period after publication of notice
- Interim Bankruptcy Rule 6011 requires court approval of notice of intended destruction of records, specifies required content of notice
- Rule 6011 also requires certification of destruction of records and method of destruction within 30 days after records have been destroyed

Other Provisions Affecting Patient Records

- New Code § 333 requires court to appoint a patient care ombudsman within 30 days of filing any bankruptcy case by or against a health care business
- Among other duties, patient care ombudsman must maintain confidentiality of patient records, prohibited from reviewing them without prior court approval, except as consistent with Older Americans Act of 1965 or state laws governing State Long-Term Care Ombudsman program

Restrictions on Disclosure of Names of Minor Children

- New § 112 restricts disclosure of the names of minor children in publicly-filed bankruptcy papers
- Debtor may not be required to disclose the names of minor children in public records

Restrictions on Disclosure of Means of Identification

- Amended § 107 protects against disclosure of identifying information affecting individuals
- Section not self-executing; debtor or party-in-interest must file motion and court must conclude that disclosure would create undue risk of identity theft or other injury to individual or his/her property

Implications of Sections 112 & 107 for Businesses

- High percentage of population implicated in domestic support obligations (DSOs)
- Preferential treatment of DSOs under BAPCPA means business debtors will have to deal with DSOs
- Business debtors may have to list individual beneficiaries of DSOs as creditors

Unsecured Creditors' Access to Information

- Amended § 1102(b)(3) requires committees to provide creditors having claims of the kind represented by committee access to information
- "Information" not defined by BAPCPA

Developments in Bankruptcy Courts

- Courts have generally shown a willingness to protect debtor's "confidential" or "privileged" information
- Some courts have provided explicit guidance on what is meant by "confidential" or "privileged" information
- Other courts have left determination to the committee

Developments in Bankruptcy Courts

- Protection for confidential information of third-parties in possession of debtor
  - Protections are still evolving
  - Some courts have conditioned disclosure of third-party data on notice to affected third-parties
  - Other courts have left issues regarding disclosure with committee

ACC 2006 Annual Meeting: The Road to Effective Leadership

Privacy & Data Security Issues Matter!

- It's not just what's in the news
  - Bankruptcy
  - Retail
  - Every business collecting PII
  - Mergers & Acquisitions (especially re: EU and Canada)
- Consider Chief Information Security Officer
- Develop Information Management Program
- Be prepared!