

The following article appeared In The Review Of Banking & Financial Services
A Periodic Review Of Special Legal Developments Affecting Lending
And Other Financial Institutions

Recent Developments In State Breach-Notification And Information Security Laws

State information security laws are becoming more stringent and prescriptive to safeguard personal information entrusted to businesses. The author discusses the California breach-notification law, which has been followed by other states, the recently issued Massachusetts revised regulation detailing minimum security standards, and some notable cases filed as a result of security breaches.

By John B. Kennedy

As the commercial significance of electronic commerce continues to grow, and as businesses of all kinds continue to amass and mine huge digital troves of consumer data, lawmakers, regulators, courts, and consumer advocates are struggling with several basic questions:

1. What obligations are owed to individuals whose personal data have been accessed or acquired by unauthorized persons, whether through negligent or intentional acts; what constitutes actionable 'harm' to such individuals?
2. What is the standard of care that private businesses should meet to protect consumer and employee data from unauthorized access and acquisition?
3. Should compliance with that standard of care be tied to particular technology implementations (e.g., the use of encryption)?
4. Should there be a single, preemptive federal standard governing the information security obligations of private businesses that experience data breaches?

John B. Kennedy is a partner in the Information Technology and Intellectual Property practice group at Dewey & LeBoeuf LLP in New York City. Mr. Kennedy gratefully acknowledges the assistance of Nathan C. Dee, an associate in the firm's New York Information Technology and Intellectual Property practice.

This article is reprinted with permission from the December 2009 edition of *The Review Of Banking & Financial Services*. © 2009 A Periodic Review Of Special Legal Developments Affecting Lending And Other Financial Institutions. All rights reserved. Further duplication without permission is prohibited.

The answers to these questions, as is often the case in matters of privacy in the United States, depend upon the type of business and nature of the data involved. Legal obligations regarding the security of personal information are largely specific to distinct industry sectors, and there is currently no comprehensive, uniform legal standard governing the obligation to protect the security of personal information held by a business.¹

Certain industry sectors – notably banking and healthcare – are already subject to detailed regulations governing the collection, use, disclosure and security of consumer data. The financial services industry’s obligations respecting information security derive largely from the Security Rule under the Gramm-Leach-Bliley Act (“GLBA”) and the various implementing regulations by the primary financial regulators under GLBA, including banking regulators and the SEC.² Even in these regulated areas, however, the legal regimes for information security compliance are still nascent and evolving. For example, the SEC’s current Regulation S-P does not provide for a breach-notification procedure and a proposed amendment to provide one generally comparable to that prescribed for banks, published by the Commission in March 2008, is still pending. Even if Regulation S-P is amended as proposed, the regulation will not necessarily oust state laws, because the GLBA specifically provides that it does not preempt state laws that provide more expansive protections for consumers.³ Since that is certainly the case now, and may continue to be so even if Regulation S-P is amended, broker-dealers, investment advisers, and investment companies are well advised to consult the information security laws of the applicable states in developing their security programs, and their response and notice plans for dealing with a security breach.

Paying close attention to state information security laws is important for several reasons. First, data breaches can be both costly and embarrassing. Corporate troves of consumer data constitute prime targets for both casual hackers and organized rings of identity thieves. There are thriving international markets in stolen credit card and other financial account and transactional data, and the advent of e-commerce has greatly expanded the opportunities for those who traffic in such markets. With some estimates showing that the average cost of a security breach to the victim business is in the millions, corporate executives have begun to realize that investments in information security assets and processes are not optional. A recent study, for example, indicates that the average all-in organization costs of a security breach in the United States is at \$6.6 million.⁴ Reflecting the business world’s increased reliance on outsourcing for data processing and storage functions, the same study notes that in 2008 breaches involving third-party providers (such as outsourcing firms) accounted for over half of all reported data breaches.⁵ Another survey of 2008 data breach incidents by Verizon underscores the overwhelming attractiveness of online data assets to hackers and cyber thieves. According to the Verizon study, 94% of the reported breaches involved online assets such as servers and applications available over the Internet, or what is increasingly referred to in the business community as “the Cloud.”⁶ The Verizon report also confirmed what is apparent in the majority of reported

-
1. The focus of this overview is limited to recent state laws and regulations directed at information security compliance practices in the private sector, in particular information security breaches, *i.e.*, protection of the confidentiality, security, integrity, and accessibility of non-public personal information from unauthorized access and acquisition (and from subsequent possible misuse in identity theft or other types of financial fraud). Laws and regulations directed to other privacy practices are outside the scope of this article.
 2. 15 U.S.C. § 680(b) (1999) (GLBA Security Rule); *see also, e.g.*, SEC Reg, S-P, 17 C.F.R. Part 248, Subpart E.
 3. 15 U.S.C. § 6807 (a), (b).
 4. Ponemon Institute LLC, 2008 Annual Study: *Cost of a Data Breach* (February 2009).
 5. *Id.*
 6. Wade H. Baker, C. David Hylender and J. Andrew Valentine, 2008 *Data Breach Investigations Report: A Study Conducted by the Verizon Business RISK Team* (2008).

security breaches: namely, that detection of security breaches is often belated and, in more than half of reported instances, does not occur until third parties have notified the victim of fraudulent activity – in other words, after the horses have well cleared the barn door.⁷

Second, the trend in the law, despite opposition from industry groups, is toward the imposition of more stringent and prescriptive baseline information security requirements derived from industry standards and from the accumulated experience of regulatory enforcers, such as the Federal Trade Commission. One of the debates presently underway in the states is over how to strike a balance between (a) reasonable private sector information technology standards for combating fraud and identity theft, and (b) cost-effective compliance requirements that are adaptable to the unique risk scenarios for each legal business and that do not lock into the law a bias for any particular security technology (such as encryption). As with information technology generally, security technology is a continuously moving target, and most policy thinking holds that no legal compliance regime should be wedded to any particular type of technology standard, nor should technological innovation in this area be distorted by laws that may become outdated soon after they are enacted. It is therefore conventional wisdom among policy makers that any laws mandating information security requirements must be “technology-neutral.” A related concern is that regulations should not burden businesses with the costs of high-test security technology when cheaper, more ‘plain vanilla’ measures could provide effective data security.

In fact, most existing laws and regulations directed to information security stress this principle of flexibility in achieving compliant information security protection. The FTC’s Safeguards Rule is the prime exemplar of this flexible, risk-based approach for determining appropriate information security measures.⁸ However, some newer state laws, discussed below, seek to impose more detailed technological requirements for minimum information security measures, including the use of firewalls, network monitoring systems and encryption.

Third, states with breach-notification laws impose specific (and potentially costly) notice and disclosure requirements for companies that experience security breaches, together with penalties for non-compliance. While the requirements imposed by these laws are by no means uniform, collectively they constitute a default national regime of security breach-notification law. Such laws are discussed below.

An Overview Of State Breach - Notification Statutes

As of September 2009, 45 states and the District of Columbia have enacted breach-notification statutes. States adding breach-notification statutes in the last 12 months include Alaska, Iowa, Missouri, South Carolina, Virginia, and West Virginia. In keeping with the tradition of state breach-notification legislation, these new laws generally follow California SB 1386, the first state breach-notification statute, which became effective in 2003.

The basic object of breach-notification laws is to mitigate risks of consumer fraud and identity theft by assuring prompt consumer awareness of unauthorized access to sensitive personal information. With knowledge of the potential exposure of personal information to identity thieves, consumers can take steps to spot fraud in their accounts and take other appropriate measures to minimize the financial harm and inconvenience of credit card fraud and/or identity theft (e.g., get a new credit card, obtain

7. *Id.*

8. 16 C.F.R. § 314 (2002).

credit watch services, impose a credit freeze on their consumer records). Essentially, each state law obligates persons (and generally, state agencies as well) that own or license “personal information” (as defined in the statute) to notify state residents when there has been a security breach in which their personal information was accessed, or reasonably believed to have been accessed, without authorization. This statutory notification obligation forces companies that are security breach victims to “go public” with the news of a security lapse affecting their customers or employees. It is argued that this disclosure obligation has had the general effect of incentivizing large consumer-oriented businesses that are prime targets of identity theft to improve their information security practices.⁹

Although state breach-notification laws are far from uniform in their requirements, all contain certain basic obligations that generally follow the terms of the original California statute. The overview below addresses those features of the California statute that have been generally adopted by 44 other states and notes some of the kinds of variations in later-adopted “copy-cat” laws.

Key Elements Of California’s Sb 1386

Covered Entities

Any organization conducting business in California and that owns or licenses computerized data that includes “personal information” must disclose any security breach where unencrypted personal information on any California resident was, or is reasonably believed to have been, acquired by an unauthorized person. The phrase “owns or licenses” is not defined in the statute but encompasses both personal information collected from customers and used in a business as well as employees of a business. The disclosure obligation is limited to (a) organizations conducting business in the state that (b) own or license “computerized data” on state residents where (c) “personal information” included in such computerized data is (or is reasonably believed to be) “acquired” by an unauthorized person. Non-computerized data are not within the reach of the statute. Personal information that is “encrypted” is also exempt from the statute’s notification requirement; this safe harbor for encryption is discussed in more detail below.

Personal Information Subject to the Breach-Notification Requirement

The California statute does not cover breaches of any and all kinds of personally identifying information, only the combination of first name or first initial and last name, together with one or more of the following: (i) Social Security number; (ii) driver’s license or state ID number; (iii) account number, credit or debit card number, in combination with security or access codes or passwords to an individual’s financial account; (iv) medical information (*i.e.*, any information regarding an individual’s medical history, mental or physical condition, or treatment or diagnosis by a healthcare professional); or (v) health insurance information (*i.e.*, an individual’s health insurance policy or subscriber ID number, any unique identifier used by a health insurer to ID the individual, or any information in the individual’s application and claims history).¹⁰ “Personal information” does not include publicly available information that is lawfully made available by federal, state, or local government records.

9. See, *e.g.*, *Security Breach Notification Laws: Views from Chief Security Officers*. A Study Conducted for the Samuelson Law, Technology & Public Policy Clinic: University of California-Berkeley School of Law (December 2007).

10. Ca. Civ. Code § 1798.82 (2003).

Other states have expanded the California definition of personal information in their breach-notification laws to include, for example, such information as biometric data, employee identification number, passport number, e-mail address, mother's maiden name, insurance policy number, and other unique numbers or identifiers.¹¹ Accordingly, the specific definition of "personal information" for each state implicated in a security breach should be consulted in determining whether notice may be required in a multi-state breach.

Encryption

Data which is stored in encrypted form is not covered by the notification requirement in California or in most other states; however, most states do not exempt encrypted data when there has also been a compromise of the encryption key. "Encryption" is undefined in some breach-notification statutes, and attempts to define it and tie compliance to its use have generated resistance and controversy. Some states employ definitions of encryption that are limited to traditional cryptography (e.g., "the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key").¹² Other states, seeking a more technology-neutral approach, use definitions of "encryption" that include existing cryptographic technologies or "another method" at least as secure.¹³ In general, however, the use of an industry standard or widely recognized method of data encryption in transmitted and stored computerized data provides a form of safe harbor for businesses that experience a breach, provided that the decrypting tools are also not compromised in connection with the breach.

Threshold of Harm and "Notice Trigger"

A critical element in all state breach-notification laws is the "notice-trigger" provision: what circumstances turn a security *incident* (i.e., an event of unauthorized access to computerized personal information) into a security *breach* requiring notice to affected individuals? Under the California statute, a breach of security gives rise to the notice obligation where unencrypted personal information on any California resident was, or is reasonably believed to have been, *acquired* by an unauthorized person. Although "acquired" is not defined, guidelines published by the state's Office of Privacy Protection indicate that acquisition should be assumed where unencrypted personal information resides on a lost or stolen device.¹⁴ Notably, a breach under the California statute does not require a determination that harm to the affected individuals is likely.

The issue of a "harm threshold" has been one of the most controversial aspects in state breach-notification legislation in recent years. Some states have implemented even broader trigger requirements than California,¹⁵ while other states have attempted to narrow the notice-trigger conditions by excusing notice where the affected organization has determined, upon investigation, that harm is not likely to result to the individuals whose personal information was compromised.¹⁶ These variations from the California approach, however, are not uniform, and accordingly there are inconsistent

-
11. See, e.g., Ark. Code Ann. § 4-110-103(5) (2005); Neb. Rev. Stat § 87-802(5) (2006); N.D. Cent. Code § 51-30-01(2)(a) (2005).
 12. Mo. Rev. Stat. § 407.1500 (2009).
 13. Mich. Comp. Laws § 445.63 (2006).
 14. California Office of Privacy Protection, *Recommended Practices on Notice of Security Breach Involving Personal Information* (2009), http://www.oispp.ca.gov/consumer_privacy/pdf/COPP_Breach_Reco_Practices_6-09.pdf.
 15. See, e.g., Conn. Gen. Stat. § 36a-701b (2006); N.J. Stat. Ann. § 56:8-163 (2005).
 16. See, e.g., Alaska Stat. § 45.48.010 (2008); Fla. Stat. § 817.5681 (2005); N.C. Gen. Stat. § 75-65 (2005).

notice-trigger provisions under the various state breach-notification laws. In the face of these inconsistencies, many businesses that experience multi-state or nationwide breach situations have opted to apply the highest notification standard applicable – often California’s – rather than limit notification to affected individuals based on a state-by-state analysis. Uniform treatment of customers according to the highest applicable breach-notice standard is normally seen as the only practical, customer-friendly response, especially in light of the potential adverse publicity were customers to be treated differently simply because of the wording of the breach-notice laws of the states where they reside.

Most state laws provide an exception to the definition of security breach for “good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business,” provided that the personal information is not used or subject to further unauthorized disclosures. Thus, for example, no security breach will be deemed to have occurred where employees or contractors inadvertently exceed their level of authorized access to a company’s data on customers or employees and are exposed to sensitive records. However, this exception may not apply where such an inadvertent exposure subsequently leads to further unauthorized acquisition of personal information (e.g., the employee who exceeded her access to personal information by taking home an unencrypted laptop then loses the laptop or shares the information with unauthorized persons outside the company).

Application to Service Providers

The notice requirement of the California statute also has limited application to a person or business that maintains computerized personal information but does not own or license such information (e.g., an outsourced data processing service provider or third-party administrator). Such entities must immediately notify the owner or licensee of the data containing personal information in the event of a breach of security as defined in the statute. Although owners or licensees of computerized personal information may delegate the execution of notice functions to such third parties, the statute’s notice obligations are not excused as a result of such delegations. Accordingly, businesses that outsource the storage or processing of personal information should conduct adequate diligence on the ability of such third-party processors to secure personal information and obtain adequate contractual safeguards and commitments in contract arrangements with third-party processors. Given the extent of the use of outsourcing in the financial services and insurance industries, many companies have developed standard data protection terms (including breach-prevention and response obligations) in their form contracts for use with external service providers.

Timing of Notice

Under the California statute, notification should be made “in the most expedient time possible and without unreasonable delay” consistent with the needs of law enforcement and measures necessary to determine the scope of the breach and to restore integrity to the data systems. Notice may be delayed pursuant to a determination by a law enforcement agency that notification will impede an investigation of the incident. Remediation of a security breach and an initial investigation of the source of the breach are recognized in all of the state breach-notice laws as first priority measures. Accordingly, no statute obligates breach victims to rush into giving notice to affected individuals before conducting internal and (where appropriate) law enforcement investigations. However, some states have begun to set more specific time requirements. For example, Florida and Ohio require notification within 45 days, depending on law enforcement approval.¹⁷ Maine recently adopted an amendment to

17. See, e.g., Fla. Stat. Ann. § 817.5681-1(b) (2005); Ohio Rev. Code Ann. § 1349.19(B)(2) (2005).

that state's breach-notification law limiting the amount of time a business or state agency may delay notification due to a pending law enforcement investigation to a maximum of seven days.¹⁸ Again, for multi-state breaches, the various states' differing notice requirements pose a challenge to businesses that seek to simplify notice compliance by using a single, uniform breach-response procedure.

Method of Notice; Content of Notice

In California, notice may be made in writing, by e-mail (if consistent with 15 U.S.C. § 7001 (E-Sign Act)), or by substitute mass notice if the cost of providing individual notice would exceed \$250,000 or the affected class of persons receiving notice exceeds 500,000. Substitute notice consists of (1) e-mail notice when an address is available, (2) conspicuous posting on the company's Web site, and (3) notice published in statewide media. Most other states allow for notification in writing or via e-mail and some have added telephone and fax notification as additional acceptable methods.¹⁹ Substitute notice is generally the same in all states, requiring e-mailing to customers, conspicuous posting on the company's Web site, and publication in major, statewide news media.²⁰ However, several states have lowered the threshold of customers affected or cost to the company to allow companies to provide substitute notice for smaller breaches.²¹

Most states, including California, require the following information in a written notification of a security breach: (a) a general description of the event; (b) the nature of the personal information accessed (*i.e.*, name, Social Security number, medical information, etc.); (c) the efforts that the entity has made to curb further unauthorized acquisition of personal information; (d) any assistance the entity is offering to affected individuals (*i.e.*, free credit-monitoring services, etc.); (e) contact information for the entity, including a toll free phone number that affected consumers can use to contact the company; and (f) information on how consumers can protect themselves, including contacts for credit reporting agencies and advice on preventing identity theft.²²

The California legislature made a number of recent attempts to amend its law to require that all breach notifications be written in plain English and contain specified information about the breach, including what information may have been breached, the date and a general description of the breach incident, the number of persons affected, and contact information for the reporting business or agency, and for all major credit reporting agencies.²³ The proposed bills would have also required businesses and agencies, in the event of a breach, to notify the Office of Information Security and Privacy Protection (OISPP). Although the proposed California bills were eventually vetoed by Gov. Schwarzenegger, other states have followed California's lead and adopted similar requirements of their own.²⁴

Notification of Law Enforcement

18. Pub. L. 2005, c. 583, § 1 (2009); Pub. L. 2005, c. 379, § 1 (Me. 2009).

19. See, e.g., Ohio Rev. Code § 1347(12) (2006).

20. See, e.g., Cal. Civ. Code § 1798.29(g)(3) (2003).

21. See, e.g., Kan. Stat. Ann. § 50-7a01-02 (2006).

22. California Office of Privacy Protection, *Recommended Practices on Notice of Security Breach Involving Personal Information* (2009), http://www.oispp.ca.gov/consumer_privacy/pdf/COPP_Breach_Reco_Practices_6-09.pdf.

23. S.B. 364, Calif. Leg., 2007-2008 Sess. (Calif. 2007); S.B. 20, Calif. Leg., 2009-2010 Sess. (Calif. 2009).

24. See, e.g. Haw. Rev. Stat. § 487N-2(d) (2006); Md. Code Ann., Com. Law § 14-3504 (2007).

California's OISPP has issued recommended practices which suggest that notification to law enforcement should only occur if the entity believes illegal activity was involved.²⁵ On the other end of the spectrum are states which require notification to law enforcement before consumer notification may occur.²⁶ In addition, more than half of the states with these laws now require notification to consumer reporting agencies when a certain threshold of affected consumers is met (ranging from 500-1,000). Many states now specifically require notification to the attorney general or another consumer protection agency.²⁷

Enforcement and Penalties

The California statute establishes a private cause of action for injured consumers and provides for injunctive relief as well. However, most state breach-notification laws allow for enforcement only by the state attorney general or the state consumer protection agency.²⁸ Many states have set up fine schedules based on the number of violations or the time it takes for companies to notify their customers. These fines range from \$10,000 – \$500,000.²⁹

Safe Harbor for Federally Regulated Entities

A number of states have provided some form of safe harbor from their breach-notification laws for entities that are subject to and in compliance with specific federal statutes or guidelines, such as the Gramm-Leach-Bliley Act or the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.³⁰ In most cases, however, these safe harbors are limited in scope and do not exempt entities completely from the notice statute requirements. For example, Colorado and Michigan exempt GLBA-compliant entities from the obligation to notify consumer reporting agencies in the event that over 1,000 residents are affected, but such entities must otherwise fully comply with the breach-notification obligations in those states.³¹ Some states merely indicate that a business will be deemed in compliance with the breach-notification requirements so long as it is regulated by a state or federal regulator and maintains procedures for an information security breach pursuant to the laws, rules, regulations, or guidelines established by such regulator.³² As of October 2009, Tennessee and Arizona are the only two states that explicitly offer a full exemption from breach-notification requirements to entities that are subject to the GLBA (regardless of whether they otherwise maintain breach-notification procedures).³³

25. California OISPP, *Recommended Practices on Notice of Security Breach Involving Personal Information* (2009), http://www.oispp.ca.gov/consumer_privacy/pdf/COPP_Breach_Reco_Practices_6-09.pdf.

26. See, e.g., N.J. Stat. 56:8-163 (2006).

27. See, e.g., Me. Rev. Stat. tit. 10, § 1348(4)-(5) (2006); N.Y. Bus. Law § 899-aa(6)(a) (2005); N.C. Gen. Stat. § 75-65(f) (2005).

28. See, e.g.; La. Rev. Stat. Ann. § 51:3075 (2006); Tenn. Code Ann. § 47-1-101 (2005); Wash. Rev. Code Ann. § 19.255.010(10) (2005); N.C. Gen. Stat. Ann § 75-65(d) (2005).

29. See, e.g., R.I. Gen. Laws § 11-49.2-6 (2005); Utah Code Ann. 13-42-301(3) (2007); Me. Rev. Stat. Ann. tit. 10, § 1349(2) (2006).

30. 12 C.F.R. § 30 *et al.* (2005).

31. Colo. Rev. Stat. § 6-1-716(d) (2006); Mich. Comp. Laws § 445.72 (2007).

32. See, e.g., Neb. Rev. Stat. § 87-804(2) (2006).

33. See Tenn. Code Ann. § 47-18-2107(i) (2005); Ariz. Rev. Stat. § 44-7501(J)(1) (2007).

State Laws Mandating Minimum Security Measures

In addition to breach-notification laws, several states have enacted statutes mandating minimum levels of security for businesses and agencies that own, license, maintain, or store personal information. Recent developments, discussed below, suggest that such laws, or the regulations and guidance that accompany them, are likely to become more specific and prescriptive as to baseline technical measures to promote data security, particularly with respect to encryption of personal information.

Most of these statutes currently require covered entities to establish and maintain practices to safeguard personal information, including requiring that they institute “reasonable” or “adequate” security procedures and practices. However, what constitutes a “reasonable” level of security is generally not defined in any detail and businesses are left to determine the appropriate standards for safeguarding the protected information. For example, any business that owns or licenses personal information about a resident of California is required to “implement and maintain reasonable security procedures and practices” to protect that information.³⁴ The particular level of security is not described, but companies are required to establish standards that are “appropriate to the nature of the information” in order to protect it from “unauthorized access, destruction, use, modification, or disclosure.”³⁵ California’s OISPP guidelines strongly recommend encryption consistent with the National Institute of Standards and Technology (NIST) standards wherever feasible.³⁶ Companies that wish to disclose personal information to unaffiliated third parties may only do so if the recipients contractually agree to implement and maintain reasonable security procedures, subject to the same level of standards applicable to the disclosing party.³⁷ The requirements of these provisions do not apply to companies that are already subject to stricter privacy standards imposed by other laws, such as the Confidentiality of Medical Information Act, the federal Health Insurance Portability and Availability Act of 1996 (HIPAA), or any other state or federal laws providing greater protection to personal information, provided that such companies are in compliance with such laws.³⁸ The statute also exempts financial institutions that are subject to the California Financial Information Privacy Act, and defines the term “financial institutions” in the same way as that term is defined under the GLBA (*i.e.*, “any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 of the United States Code...”).³⁹

In Nevada, any business entity or association that maintains personal information about a Nevada resident must also implement and maintain “reasonable security measures” to protect such information from “unauthorized access, acquisition, destruction, use, modification, or disclosure.”⁴⁰ However, Nevada recently has become one of the first states with a mandatory encryption law. Since October 1, 2008, Nevada businesses have been prohibited from transferring “personal information of a customer through an electronic transmission other than facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.”⁴¹

34. Cal. Civ. Code § 1798.81.5(b) (2006).

35. Cal. Civ. Code § 1798.81.5(b) (2006).

36. California Office of Privacy Protection, *Recommended Practices on Notice of Security Breach Involving Personal Information* (2009), http://www.oispp.ca.gov/consumer_privacy/pdf/COPP_Breach_Reco_Practices_6-09.pdf.

37. Cal. Civ. Code § 1798.81.5(c) (2006).

38. Cal. Civ. Code § 1798.81.5(e) (2006).

39. Cal. Fin. Code. § 4052(c) (2004).

40. Nev. Rev. Stat. § 603A.210(1) (2006).

41. Nev. Rev. Stat. § 597.970(1) (effective October 1, 2008).

Nevada recently amended its encryption statute to require encryption of personal information found on data storage devices that are moved outside the physical and logical controls of the data collector. The amendment defines “data storage device” as “any device that stores information or data from any electronic or optical medium, including, but not limited to, computers, cellular telephones, magnetic tape, electronic computer drives, and optical computer drives.” The revised Nevada law also expands the definition of “encryption” to require covered entities to use both of the following: (i) an accredited encryption technology that has been adopted by a standards-setting body such as the Federal Information Processing Standards and (ii) other appropriate management and safeguards of cryptographic keys using guidelines established by NIST. Finally, the new law requires entities that accept credit cards to comply with the Payment Card Industry Data Security Standard, or otherwise be liable for damages in connection with an information security breach.⁴²

The Massachusetts Information Security Regulations

A key venue for the current debate over legally mandated data security requirements is Massachusetts. In 2008, the Massachusetts Office of Consumer Affairs and Business Regulation (“OCABR”) proposed a comprehensive regulation, 201 CMR 17.00, establishing detailed minimum security standards to be met in connection with the safeguarding of personal information of Massachusetts residents. The proposed regulation has subsequently been the subject of considerable pushback by the business community, has been debated in public hearings, revised, delayed in its enforcement on three separate occasions, and was recently rewritten (again) and shortened by OCABR in an attempt to respond to public criticism. The modified Massachusetts regulation is now set for implementation on March 1, 2010.

The debate surrounding the Massachusetts security regulation is noteworthy because it encapsulates the current nationwide legislative struggle to impose workable standards for information security in the face of a continually changing information technology environment and the increasingly sophisticated tactics of those who seek to steal digitized personal information held by private businesses and government.⁴³ In particular, the Massachusetts regulation has focused the debate on how prescriptive and detailed information security regulations can or should be.

The key aspects of the Massachusetts regulation, as originally proposed, included broad administrative requirements familiar to banks already subject to GLBA. For example, every person that owns, licenses, stores, or maintains personal information about a Massachusetts resident must implement and maintain a comprehensive, written information security program that is reasonably consistent with industry standards and contains administrative, technical and physical safeguards to ensure the security and confidentiality of such information.⁴⁴ The jurisdictional sweep of this requirement – poten-

42. S.B. 227, 75th Leg., Reg. Sess. (Nev. 2009). The Payment Card Industry Data Security Standard, which can be located at <https://www.pcisecuritystandards.org>, is a comprehensive set of requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures designed to help organizations proactively protect customer account data.

43. Martha Kessler, *Massachusetts Extends Comment Period For Proposed Personal Data Protection Rules*, PRIVACY LAW WATCH, Jan. 15, 2008.

44. See OCABR, *201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth* (2008) available at <http://www.mass.gov/?pageID=ocatermina1&L=4&LO=Home&L1=Consumer&L2=Privacy&L3=Identity+Theft&sid=Eoca&b=terminalcontent&f=reg201c17&csid=Eoca>.

tially reaching any entity that maintains personal information on a Massachusetts resident regardless of whether or not the entity is doing business in Massachusetts – has become part of the controversy associated with the regulation.⁴⁵

At a minimum, to be in compliance with the originally proposed regulation, an information security program must include, but shall not be limited to:

1. designating one or more employees to oversee implementation and maintenance of the program;
2. identifying and assessing internal and external risks to the security and integrity of personal information, and evaluating and improving the current safeguards for minimizing such risks, including: (a) ongoing employee training; (b) monitoring employee compliance with internal policies and procedures; (c) upgrading network, system and software information systems; (d) storage of records and data in locked facilities; and (e) improving the means for detecting, preventing, and responding to security failures;
3. developing security policies for employees who telecommute;
4. imposing disciplinary measures for violations of the security program;
5. preventing terminated employees from accessing personal information;
6. taking reasonable steps to verify that all third-party service providers are capable of maintaining safeguards for protecting personal information, and contractually requiring such service providers to maintain such safeguards;
7. collecting the minimum amount of personal information necessary, maintaining it for the minimum amount of time necessary, and permitting access to the smallest number of people necessary in order to accomplish the purpose for which it was collected;
8. inventorying records, computer systems, and storage media to identify those records containing personal information;
9. regularly monitoring and auditing employee access to personal information;
10. reviewing the scope of the security program at least annually or whenever there is a material change in business practices; and
11. documenting responsive actions taken in connection with any security breach, and establishing procedures for a mandatory post-incident review of events to make any necessary changes in business practices relating to protection of personal information.

45. Barbara Yuill, *Massachusetts Officials Discuss Security Rule at Conference, Give Compliance Advice*, Privacy Law Watch, Sept. 21, 2009.

For banks subject to regulation under GLBA and its implementing regulations, the above requirements are not radically new or different than those in existing GLBA regulations and agency guidelines. For securities firms, the requirements go far beyond those of regulation S-P. In addition, the Massachusetts regulation provides that enforcement will be flexible and gauged to the size and nature of the particular business and of the risk. That is, the adequacy of an information security program shall be evaluated taking into account: (a) the size, scope and nature of business of the person implementing the program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality. In other words, OCABR will not expect a business with 50 employees to have an information security program worthy of a Fortune 500 company.

The revised version of the Massachusetts regulation, issued in August 2009, retrenches some of the administrative requirements listed above. For example, the requirement to “verify” third-party data processors’ compliance with the regulation has been modified to allow businesses to renegotiate non-compliant contracts up until March 1, 2012 (so long as these were entered into prior to the regulation’s effective date of March 1, 2010). The requirement of inventorying records and computer systems – a potentially expensive exercise in data-mapping – has also been dropped. However, the revised regulation continues to apply to all persons that own or license personal information about Massachusetts residents, a feature that may prompt dormant Commerce Clause challenges once the regulation becomes effective.

The most controversial features of the Massachusetts regulation, however, have been the computer system security requirements. As originally proposed in 2008, these requirements had a level of specificity and prescriptiveness unprecedented in similar state laws. Key requirements under the original wording of the regulation include: (a) detailed secure user-authentication protocols; (b) secure access control measures; (c) encryption of all transmitted files containing personal information that will travel across public networks; (d) periodic monitoring of networks and systems for unauthorized use or access, and recording of audit trails and periodic review of audit trails; (e) implementation of a firewall with up-to-date patches that must, at a minimum, protect devices containing personal information from unauthorized use or access; (f) installation of the most current version of system security software including antispymware and antivirus software; (g) education and training of employees on the proper use of the computer security system and the importance of personal information security; and (h) restricted physical access to computerized records containing personal information, and a review of the integrity of such records upon learning of any unauthorized entry into a secure area by an unauthorized employee or other person.

Under the August 2009 revised regulation, some of the technology-specific provisions in the original have been removed, while others have been enhanced. For example, the revised regulation removes the requirement of using “the most current version” of security-related software (replacing that concept with the term “reasonably up-to-date versions of system security agent software”), but, on the other hand, the encryption requirement for transmissions now includes all transmissions of personal data by wireless means (whether on an internal network or otherwise). In general, the more prescriptive terms of the original regulation have been qualified to require “reasonable” measures. Moreover, under the original regulations, covered entities were required to obtain written certification from third-party service providers (TSPs) with access to personal information that such TSPs had comprehensive information security programs in place, and to contractually obligate TSPs to maintain safeguards for the protection of personal information. The revised regulations eliminate the require-

ment regarding written certification (although covered entities are still obligated to reasonably verify that TSPs are capable of protecting personal information and to contractually obligate TSPs to maintain safeguards for the protection of personal information).⁴⁶

Even with these revisions, 201 CMR 17.00 represents a significant expansion of previous state information security requirements. At least nine other states – Arkansas, California, Connecticut, Maryland, Nevada, Rhode Island, Oregon, Texas and Utah – mandate minimum security requirements for businesses that store personal information, but, to date, all stop short of Massachusetts' detailed list of minimum requirements.⁴⁷

At present 201 CMR 17.00, as revised, is set for enforcement as of March 1, 2010. Barring further revisions to the regulation that narrow its scope or dilute its requirements, legal challenges appear to be likely. However, for nationally based financial institutions that have already taken measures to comply with the letter of GLBA's Security Rule and to adopt security practices consistent with guidance issued by GLBA's regulators, the new Massachusetts regulation should not represent dramatic change nor require significant new technology investments. The more-likely aggrieved businesses affected by the regulation will be large, non-regulated enterprises that have only tangential contacts with Massachusetts. Even if Massachusetts is found to have overstepped its authority by improperly burdening interstate commerce with this regulation, the trend toward greater prescriptiveness and specificity in information security regulations is likely to continue.

Enforcement Actions And Civil Litigation

A FINRA Enforcement Action

A recent enforcement action by the Financial Industry Regulatory Authority ("FINRA") indicates how some financial services businesses can be subject to both state and federal information security requirements. In April 2009, FINRA announced that California-based Centaurus Financial, Inc. had agreed to pay a \$175,000 fine following a security breach of its fax server through a phishing scam which had enabled hundreds of unauthorized log-ins to the server and access to sensitive Centaurus customer account information (including account numbers and Social Security numbers). Centaurus had previously sent notice of the incident to 1,400 affected customers pursuant to state breach-notice laws, but, according to FINRA, this notice compounded the problem by providing a misleading description of the security breach that understated the nature and extent of the breach (e.g., part of the vulnerability was due to Centaurus using default, vendor-supplied passwords on the affected server). FINRA alleged that both the security practices underlying the breach and the inadequate customer notice letter were violations of SEC Regulation S-P and FINRA rules.⁴⁸

46. 201 C.M.R. 17.00 (Mass. 2009).

47. Thomas J. Smedinghoff and Laura E. Hamady, *New State Regulations Signal Significant Expansion Of Corporate Data Security Obligations*, *Privacy Law Watch*, Oct. 21, 2008.

48. See FINRA press release at <http://www.finra.org/Newsroom/NewsReleases/2009/P118550>. FINRA is authorized to impose sanctions on member organizations for violations of federal securities laws, rules, and regulations pursuant to Rule 8310 of the FINRA Manual.

State Enforcement Actions

State attorneys general have begun enforcing breach-notification laws. In 2007, for example, the New York State Attorney General reached the state's first settlement with CS STARS LLC, when that company waited seven weeks to report that a laptop with private information had been stolen by a janitorial worker. As part of the settlement, the company agreed to improve its security program, to be more responsive if a future breach occurs, and to pay the Attorney General \$60,000 to reimburse the state for the cost of the investigation.⁴⁹ In 2006, the North Dakota Insurance Commissioner ("NDIC") entered into a settlement with Humana Insurance Company in connection with two isolated incidences of theft of Humana policyholders' private financial information, including names, addresses, Social Security numbers and bank routing information. The NDIC claimed that Humana failed to notify it of the breach in accordance with the North Dakota statute, which requires regulated entities to notify their primary regulators. As a result of the settlement with the NDIC, Humana was required to provide two years of free credit monitoring for residents affected by the breach, and to pay the NDIC for costs incurred while investigating the incidents.⁵⁰

In a more recent state enforcement action, the Bank of New York Mellon (BNY) and the Connecticut Department of Consumer Protection and the Department of Banking signed an Assurance of Voluntary Compliance (AVC) in January 2009 following the loss of a back-up storage tape which contained personally identifiable information. The state directed BNY to notify each affected bank customer and to provide 24 months of credit protection for the financial accounts that might be affected by the data breach. Additionally, under the AVC, BNY was required to provide an additional year of credit monitoring to individuals who were notified late, as well as cover any actual losses suffered by individuals as a result of the breach. BNY has further provided identity theft insurance in the amount of \$25,000 reimbursement for the costs of implementing security freezes on individual accounts, and has maintained toll-free customer care numbers.⁵¹ In another Connecticut action, Bank of America agreed to pay Connecticut \$350,000 and reimburse residents for the cost of credit freezes they obtained after an employee of Countrywide stole personal data of approximately 2 million customers nationwide (including about 30,000 Connecticut residents). The AVC also requires Countrywide to adopt best practices for data management and security.⁵²

Civil Litigation

In recent years, plaintiffs have asserted various theories of liability against companies that have experienced a breach of security, including breach of contract, breach of fiduciary duty, and negligence, as well as various state and federal statutory claims. However, plaintiffs in such suits have generally failed to persuade courts of plaintiffs' injuries or establish damages based merely upon the unauthorized theft or loss of personal information. In a series of decisions in the last few years involving lost or stolen laptops, data tapes, and other security breaches, courts have adopted the view that an increased risk of future injury from identity theft exposure is insufficient to support an actionable injury or to establish damages. In particular, courts have repeatedly rejected efforts by plaintiffs to analogize

49. John B. Kennedy, *A Primer on Key Information Security Laws in the United States*, in Ninth Annual Institute on Privacy & Security Law 117 (Practising Law Institute ed., 2008).

50. *Security Breach Settlement Requires Humana to Offer Two Years of Monitoring*, Privacy Law Watch, Nov. 3, 2006.

51. Press Release, Connecticut Department of Banking, *Department of Consumer Protection and Department of Banking Announce Settlement with Bank of New York Mellon for 2008 Data Breach* (Feb. 3, 2009), <http://www.ct.gov/dob/cwp/view.asp?a=2245&q=433242> (last visited Mar. 11, 2009).

52. Press Release, Connecticut Attorney General's Office, *Attorney General, DCP Announce \$350,000 Countrywide Data Breach Settlement, Reimbursement To Nearly 30,000 CT Consumers For Credit Freezes* (Jan. 29, 2009), <http://www.ct.gov/ag/cwp/view.asp?A=3673&Q=432774> (last visited Mar. 11, 2009).

risk of future credit card fraud to the harm recognized by courts for the costs of medical monitoring of injuries or latent medical harm. In those instances where the court found a special relationship or fiduciary duty to the plaintiff with respect to the custody of personal information, some courts have allowed cases to proceed.⁵³

A few recent cases provide a representative sampling of the fate of most breach-notice plaintiffs to date. In *Randolph v. ING Life Insurance and Annuity Co.*,⁵⁴ plaintiffs participating in an ING-administered deferred compensation program alleged that an ING representative copied company files containing their personal information onto a home computer that was later stolen in a home burglary. They asserted claims against ING for invasion of privacy, negligence and breach of fiduciary duty or of a confidential relationship, and sought recovery on the grounds that the theft created a risk of future harm that prompted or may prompt them to purchase credit monitoring services. The court found the allegations insufficient to amount to an injury in fact. The court reasoned that “concrete and particularized” or “imminent” injury must exist for a successful claim. Similarly, *Kahle v. Litton Loan Servicing LP*⁵⁵ arose out of a theft of password-protected hard drives containing consumer personal information from defendant’s facility. After the break-in, the defendant provided written notice to each person whose information was contained on the hard drives and recommended that those persons place a fraud alert on their credit files. The only harm suffered by plaintiffs was the cost incurred in purchasing credit-monitoring services. The court dismissed the lawsuit in its entirety, ruling that such claims cannot withstand summary judgment where the only injury arguably suffered is the mere fear of future identity theft. A similar outcome was reached in *Pisciotta v. Old Nat. Bancorp.*,⁵⁶ which arose out of a security breach at a facility hosting the defendant bank’s online transactional Web site. More recently, the United States District Court for the Southern District of New York threw out state law claims against J.P.Morgan Chase, N.A. arising out of the loss of 2.6 million card records, in part, on the grounds that the mere possibility of data misuse does not amount to a statement of cognizable harm based on a data breach.⁵⁷ In a similar class action involving a breach at the Hannaford Bros. grocery chain, the United States District Court for the District of Maine dismissed all but one claim on the grounds that customers could not seek any damages because the breach did not result in any actual

53. The following cases are generally representative of the results in case law to date for liability to consumers affected by a data security breach. *Bell v. Acxiom Corp.*, 2006 U.S. Dist. LEXIS 72477 (E.D. Ark. 2006), holding that the plaintiff’s allegation failed to meet the Article III standing requirement of a concrete or particularized harm because it merely asserted a potential future injury rather than an injury-in-fact; *Key v. DSW Inc.*, 454 F. Supp. 2d 684 (S.D. Ohio 2006), rejecting the plaintiff’s attempt to analogize the need for credit monitoring in security breach cases to the need for medical monitoring in product liability cases, in which imminent harm arising from a defective device implanted in a plaintiff’s body, or from a plaintiff’s exposure to toxic chemicals, may meet federal standing requirements; *Forbes v. Wells Fargo Bank N.A.*, 420 F. Supp. 2d 1018 (D. Minn. 2006), holding that the cost of engaging credit monitoring services does not constitute an injury-in-fact; *Walters v. DHL Exp.*, 500 F. Supp. 2d 1007 (C.D. Ill. 2007), where the court dismissed the plaintiff’s claim for damages based on an increased risk of future identity theft but noted that the plaintiff could have made a claim under the general state tort law; *Remsburg v. Docusearch, Inc.*, 149 N.H. 148 (2003), holding that a private investigator owed a duty to exercise reasonable care to not subject a third party to an increased risk of criminal misconduct, including stalking and identity theft; *Bell v. Mich. Council*, 2005 Mich. App. LEXIS 353 (2005), holding that the union had a special relationship with its members giving rise to a duty to safeguard personal data that the members entrusted to the union; among the distinguishing facts cited by the court in finding a duty imposing relationship were the union’s obligation to act in the best interests of its members, the foreseeability (under the circumstances) of theft and misuse of the data, and the union’s lack of safeguards to prevent unauthorized access to members’ personal data; *Guin v. Brazos Higher Educ. Serv. Corp., Inc.* 2006 U.S. Dist. LEXIS 4846 (D. Minn. 2006), noting that neither the GLB Act nor its implementing regulations require data encryption during storage or transit by a regulated entity.

54. 486 F. Supp. 2d 1 (D.D.C. 2007).

55. 486 F. Supp. 2d 705 (S.D. Ohio 2007).

56. 499 F.3d 629 (7th Cir. 2007).

57. *Willey v. J.P.Morgan Chase, N.A.*, S.D.N.Y., No.1:09-cv-01397-CM, dismissed 7/7/09.

or substantial loss of money or property;⁵⁸ however, the Court recently reconsidered the case and decided to certify to the Maine Supreme Judicial Court the question of whether a person's reasonable time and effort spent on averting reasonably foreseeable harm is sufficient to constitute a cognizable injury under Maine common law.⁵⁹

In what could be one of the largest data breaches to date, a payment card transaction processing company, Heartland Payment Systems, announced on January 20, 2009, that its processing system had been compromised by malicious software in 2008. The New Jersey-based Heartland is one of the nation's top payment cards processing companies, handling card transactions worth over \$4 billion per year for restaurants and retailers. The type of information exposed included credit card numbers, expiration dates, other information from magnetic strips, and, in some cases, individuals' names who used their cards in Heartland's merchant client stores. Over 560 financial institutions of all sizes in the U.S., as well as Bermuda, Canada, and Guam, are reported to have been directly affected by the Heartland breach. Numerous data breach actions have already been filed.⁶⁰ In August 2009, Heartland filed a Form 8K disclosure with the SEC indicating that the company faced \$32 million in expenses for the first half of the year as a result of the data breach.⁶¹

Pending Federal Legislation

As the number of state breach-notification laws has grown, some business groups have called for a uniform federal approach in order to simplify compliance and preempt multiple conflicting breach-notice requirements with a single standard. For several years running, breach-notification and data security bills have been introduced in the House and Senate and then languished in committee. Presently, several of the earlier bills have been reintroduced and updated. Senate Bill 136, the "Data Breach Notification Act", was reintroduced in January 2009 by Sen. Dianne Feinstein (D-Calif.). The bill would impose a breach-notification requirement on federal agencies and businesses engaged in interstate commerce that use, access, or collect sensitive, personally identifiable information; the bill also requires such agencies or businesses to notify the U.S. Secret Service if more than 10,000 individuals are affected by a breach, if a breached database holds more than 1 million records or is a federal government database, or if the database holds national security or law enforcement data. Also among the reintroduced bills in the current congressional session is Senator Patrick Leahy's (D-Vt.) "Personal Data Privacy and Security Act" (S. 1490). As with other pending congressional bills, S. 1490 would enact a federal breach-notification scheme that would preempt conflicting state law as applicable to private businesses. Additional regulations would apply to data brokers and be enforced by the FTC. No private right of action would be created, and enforcement by federal or state officials could lead to fines of up to \$1 million per violation.

In view of the consuming healthcare debate in Congress in late 2009, it appears doubtful that a federal breach-notification law will be passed this year. The existence of 45 state laws, despite the differences among them, appeared to have slowed lobbying for federal legislation. Another reason for this may be that large businesses have been simplifying their compliance planning by adopting a "highest-applicable standard" approach to state breach-notice laws, resulting in a de facto national

58. *In re Hannaford Bros. Co. Customer Data Security Breach Litigation*, 613 F. Supp. 2d 108 (D. Maine 2009).

59. *In re Hannaford Bros. Co.*, 2009 U.S. Dist. LEXIS 92888 (D. Maine 2009).

60. See, e.g., *Lone Summit Bank v. Heartland Payment Systems, Inc.*, No. 3:09-cv-00581-FLW-TJB (D.N.J. Feb. 6, 2009); *Tricentury Bank v. Heartland Payment Systems*, No. 3:09-cv-00697-FLW-TJB (D.N.J. Feb. 13, 2009).

61. Available at: <http://www.snl.com/Cache/8155202.pdf?O=3&IID=4094417&OSID=9&FID=8155202> (last visited Oct. 7, 2009).

standard that is more or less aligned with the California statute. Another is that the Federal Trade Commission has assumed a significant role in pursuing information security practices that it deems “unfair and deceptive” under Section 5 of the FTC Act. In the last few years, the FTC has brought over 20 enforcement actions for lax information security resulting in consent decrees. In some of these cases, the FTC has alleged that a company deceptively misrepresented to its customers the extent of its security measures. In other cases, the FTC alleged that the deficient security measures, even without deceptive messages to consumer, constitute an unfair practice.⁶² The new FTC Chairman, Jon Leibowitz, has publicly reaffirmed the Commission’s focus on enforcement actions in cases of lax corporate data security, suggesting that the FTC will continue to be on the forefront of defining what constitutes inadequate information security practices.

Conclusion

Businesses that experience multistate breaches of data security must contend with the 45 (at current count) state breach-notice laws. Although regulated financial institutions that are compliant with data security requirements under GLBA and its implementing regulations generally enjoy a partial safe harbor under these state laws, such institutions must still give notice consistent with the breach-notification requirements of state law and should have breach-response programs that meet the requirements of those states on whose residents they maintain covered personal information. In addition to the now virtually national scope of non-uniform state breach-notification laws, some states are beginning to establish baseline technological security measures, either as mandated elements of compliance programs or as statutory safe harbors. The trend in this respect is towards more detailed and prescriptive requirements for making lost or stolen data unusable (e.g., through encryption) pursuant to recognized industry standards, such as NIST data security standards. If federal legislation for private sector information security does come about, it is likely to address this technology standards issue in ways designed to be “technology-neutral” and flexible according to actual levels of risk. Notwithstanding that civil litigation against businesses that suffer security breaches so far has not yielded significant plaintiffs’ damage awards (in large part because courts have not found actionable harm in the mere anticipation of identity theft), the out-of-pocket costs of security breaches (including notice costs, fines, investigations and defense of litigation) typically run in the millions for mid-sized to large data breaches. Accordingly, a comprehensive and periodically updated program of breach prevention and response should be a part of the written information security programs of businesses at risk from data breaches.

62. FTC Privacy Initiatives - Unfairness & Deception Enforcement Cases, *available* at http://www.ftc.gov/privacy/privacy_initiatives/promises_enf.html.

This article is intended only as a general discussion of these issues. It is not considered to be legal advice. We would be pleased to provide additional details or advice about specific situations. For additional information on this important topic, please feel free to call upon your Dewey & LeBoeuf relationship partner.

No part of this publication may be reproduced, in whole or in part, in any form, without our prior written consent.

© 2009 Dewey & LeBoeuf LLP
All rights reserved.

For further information on Dewey & LeBoeuf, please visit www.dl.com

8462 REV01 12-29-2009

The Review of Banking & Financial Services

General Editor

Michael O. Finkelstein

Board Members

Roland E. Brandel
Morrison & Foerster LLP
San Francisco, CA

H. Rodgin Cohen
Sullivan & Cromwell LLP
New York, NY

Carl Felsenfeld
Professor of Law
Fordham Law School
New York, NY

Ralph C. Ferrara
Dewey & LeBoeuf LLP
Washington, DC

Connie M. Friesen
Sidley Austin LLP
New York, NY

Associate Editor

Sarah Strauss Himmelfarb

Robert M. Kurucz
Morrison & Foerster LLP
Washington, DC

C.F. Muckenfuss, III
Gibson, Dunn & Crutcher LLP
Washington, DC

Morris N. Simkin
Carter Ledyard & Millburn LLP
New York, NY

Brian W. Smith
Latham & Watkins LLP
Washington, DC

Thomas P. Vartanian
Fried, Frank, Harris, Shriver & Jacobson LLP
Washington, DC