Wall Street LAWYER
Securities in the Electronic Age

November 2006, Vol. 10 No. 11

THOMSON

IN THIS ISSUE:

WEST LEGALworks

Responding to Data Breaches in the Securities and Investment Management Industry

By Steven W. Stone & Shauna R. Sappington

Steven W. Stone is a partner and Shauna R. Sappington is an associate in the Washington, D.C. office of Morgan, Lewis & Bockius LLP. All rights reserved. This article provides general information on the subject matter discussed and it should not be relied upon for legal advice on any matter. Contact: sstone@morganlewis.com or ssappington@morganlewis.com.

Scarcely a week passes without a report of a data breach involving yet another venerated financial institution or financial services company, let alone a governmental agency or securities self-regulatory organization (SRO).[1] According to a 2006 Global Security Survey conducted by Deloitte Touche Tohmatsu, 82% of the firms responding experienced a data breach within the past year.[2] All told, there have been over 250 data breaches reported so far this year, and the total number of records containing sensitive personal information involved in reported security breaches now exceeds ninety-five million.[3] Although the vast majority of data breaches do not involve identity theft or fraud,[4] recent reports describe a growing threat of hackers seeking access to customer accounts for manipulative or other fraudulent purposes.[5]

Broader concerns with protecting customer information have prompted most states to adopt a variety of data breach notification requirements, imposing on securities and investment management firms (among other businesses) a burden to comply with differing (and sometimes conflicting) requirements. These same concerns have also impelled Congress to take up data breach notification legislation to protect customer information while creating a uniform national standard for responding to data breaches, as well as the SEC to consider rule making in the area. This article discusses how securities and investment firms can prepare for and respond to data breaches in the current environment of unfolding regulatory requirements in the area.

A Medley of State Notification Requirements

Protecting nonpublic information has become the focus of a majority of states. Today, 34 states, and one municipality—New York City, have adopted varying data breach notification laws requiring firms to alert customers of security breaches involving their nonpublic personal information.[6] Problematically, these state laws require firms to either comply with conflicting state notification standards or apply the strictest state standard. In many cases, states define data breaches in different terms and impose different customer notification requirements. For example, all states have adopted notification requirements that define

[Continued on page 3]

Letter From the Editors

November – the time of the year when we put away our spooky Halloween costumes and begin thinking about defrosting the turkey. But before we do, let's have one last Treat that might help our readers deal with all the Dirty Tricksters out there.

In the top story in this issue of Wall Street Lawyer, Steven W. Stone and Shauna R. Sappington of Morgan, Lewis & Bockius LLP, fill our heads with scary tales of data breaches and how they can cripple a securities firm.

From assembling a rapid response team to deal with computer hackers and identity theft to notifying customers or regulators about the loss of confidential information, the authors describe what companies can do to guard against data breaches and what the government may be doing in the future to address the situation.

Definitely, an important read in today's environment.

Also in this issue, we begin looking at the activity swirling around the Second Circuit Court of Appeals' decision in AFSCME v. AIG, which could potentially open the floodgates for aggressive shareholder groups to gain a much stronger access to the mechanics of voting for corporate directors. The decision, which runs counter to years of SEC Staff interpretation, will be the focus of the SEC's December meeting. Wall Street Lawyer will keep its readers updated with news and analysis of this situation as it goes forward.

Also worth noting is the article by Andrew S. Tulumello and Henry C. Whitaker of Gibson, Dunn & Crutcher LLP that takes up the problem of today's prolix securities fraud complaint, which the authors describe as "a monster", often spanning hundreds of pages. Their solution: More aggressive use of Federal Rule of Civil Procedure Rule 8(a), which requires such filings to be "plain" and importantly, "short."

And as always, if there is a topic that you feel needs our coverage, please contact us; and, if anyone has a comment or a story idea for Wall Street Lawyer, drop us a line. Please send all correspondence to our Managing Editor Gregg Wirth at gregg@gwirth.com.

— John Olson and Gregg Wirth

THOMSON™

Wall Street Lawyer

West Legalworks
395 Hudson Street, 4th Floor
New York, NY 10014

One year subscription, 12 issues, $425
(ISSN: 1095-2985)

Please address all editorial, subscription, and other correspondence to the managing editor at gregg@gwirth.com.

continued from page 1

a data breach as the unauthorized access to unencrypted data, thereby, not requiring notification if the data breach involved encrypted data. However, some states do require notification if the encryption key accompanies the data.[7] Further, some state laws include a provision exempting a firm from customer notification if, after conducting an investigation, the firm determines that there no reasonable likelihood of harm or risk to customers resulting from the data breach.[8] As a result, if a firm services clients in states that provide the exemption, as well as states that do not, the firm will be required to report the data breach to some but not all of its customers.

Federal Legislation Pending

Congress is considering several bills that will establish a national approach to data protection and data breach notification.[9] In particular, the Financial Data Protection Act of 2005, supported by the SIA, would offer firms a nationally uniform notification process[10] and provide clarity to consumers regarding their privacy rights. Specifically, the Financial Data Protection Act would require notification if a "consumer reporter"[11] determines that a breach "is reasonably likely to have occurred with respect to sensitive financial identity and sensitive financial account information and such information is reasonably likely to be misused in a manner causing substantial harm or inconvenience to the consumer."[12] In contrast, the Cybersecurity Enhancement and Consumer Data Protection Act of 2006 requires that the firm notify the U.S. Secret Service or the FBI within two weeks from when the firm discovers a major breach.[13] In such instances, the firm may not notify customers of the data breach until permitted by the U.S. Secret Service or the FBI.

Despite the appeal of a national standard that would preempt inconsistent state requirements, Congress does not appear close to enacting a data breach notification law. The vast differences between the various data breach notification bills has led some proponents of data breach notification to believe that Congress will not pass a uniform standard until the 2007 legislative session. In the meantime, securities and investment management firms should continue to assess their practices and adjust their policies and procedures accordingly as additional states adopt new data breach notification laws.

Guidance from Financial Regulators

Federal banking regulators, jointly as the Federal Financial Institutions Examination Council, issued cohesive guidelines (FFIEC Guidance) in 2005 for financial institutions to follow when preparing for and responding to data breaches.[14] Specifically, the FFIEC Guidance states that each financial institution should establish a program to respond to data breaches. The FFIEC Guidance further clarifies that a firm's response program should address how to assess a data breach, notification of federal regulators, controlling the breach to reduce the risk of additional customer harm, and how to notify affected customers. Specifically, the FFIEC Guidance requires a financial institution to notify customers when the firm discovers unauthorized access to sensitive customer information that has been or is reasonably likely to be misused. The FFIEC Guidance offers a coherent set of principles upon which securities and investment management firms may want to build when developing their own plans for responding to data breaches.

SEC Action Expected

The SEC and the SROs have yet to issue guidance on how securities and investment management firms should respond to data breaches, but they are actively monitoring the area and are expected to act soon. Specifically, the SEC has been conducting examinations to better understand how broker-dealers and investment advisers are seeking to protect customer information and comply with Regulation S-P. The SEC is expected to propose rulemaking in this area in the near future.[15]

Regulation S-P, which governs the handling of nonpublic financial information of customers of broker-dealers, investment advisers and investment companies, does not itself address how firms should notify customers of or otherwise respond to data breaches. Rather, Regulation S-P requires these firms to adopt written policies and procedures designed to institute administrative, technical and physical safeguards for sensitive customer information. In 2005, the NYSE and NASD (which recently suffered its own data breach[16]) issued guidance reminding member firms of their obligations to comply with Regulation S-P.[17]

Preparing for Data Breaches

Securities and investment management firms should consider planning for possible data breaches in advance of any specific requirements from the SEC or the SROs, if only to provide for compliance with applicable state notification requirements.

- *Data Breach Policies and Procedures.* Firms should consider incorporating within their policies or procedures under Regulation S-P provisions dealing with the handling of data breaches, including a process for detecting data breaches and informing firm decision makers so they may act. As with any policies and procedures, these data breach policies or procedures should be tailored to the particular business, particularly since the needed level of detail and operational complexity will vary substantially from organization to organization.
- *Data Breach Assessment.* Firms should consider conducting data breach assessments to evaluate the circumstances that pose data breach risks. Such assessments might include an evaluation of whether firm personnel and third parties with whom the firm works have access to customer nonpublic data (*e.g.,* social security numbers) that is not necessary given their functions or responsibilities. This assessment might also consider the adequacy of firm practices to safeguard nonpublic

personal information of customers, including through appropriate protocols for the use of removable media (*e.g.,* laptops, portable hard drives, CDs, DVDs and USB drives) and use of encryption technology.

- *Assess Vendor Arrangements and Documentation.* Firms should review any arrangements they have with third party vendors that have access to personal nonpublic information of firm customers. The review should include assessing the vendor's own policies, procedures and practices relating to data breaches and the vendor's contractual or other obligations to alert the firm of data breaches.

- *Rapid Response Team.* Firms should consider designating a "rapid response" team that includes personnel from technology, compliance and legal departments. This team should be responsible for evaluating the risks of data breaches in the firm and the firm's preparedness for handling data breaches. If a data breach occurs, this team should promptly assemble to gather the facts and decide on a response plan.

- *Consider Prospective Disclosure of Data Breach Policy.* Firms may also want to consider disclosing in their privacy policies information about their policies or procedures for handling data breaches, including that they will disclose data breaches involving customer nonpublic information to the extent provided by law. If a firm's customer notifications may vary by customer because of differing regulations that apply to the customer's accounts, the firm may consider disclosing that practice. Similarly, a firm may wish to disclose that customer notification may be delayed where appropriate for the firm to cooperate with appropriate law enforcement agencies.

Ten Steps for Responding to Data Breaches

Beyond planning and establishing data breach policies and procedures, there are a number of practical steps securities and investment management firms should take to respond to data breaches when they occur.

1. *Assess the Breached Information*. The firm should identify the type of information breached (*e.g.,* account numbers, social security numbers, names or passwords), whether the information was sensitive or nonpublic,[18] and the customer accounts involved. Evaluating this information will be crucial for determining how the firm should respond, mitigate further damage and assess its notification obligations.

2. *Mitigate Further Risk to Customer Information*. The firm should investigate the cause of the breach and take any necessary action to reduce the risk of further data breaches. This may include changing account numbers, creating surveillance reports to monitor for suspicious activity, and securing servers, among other steps.

3. *Assess the Need to Alert Law Enforcement Agencies and File a Suspicious Activity Report*. The firm should evaluate whether to alert the FBI or other appropriate law enforcement agencies of any data breach that may involve or create a substantial risk of criminal activity and the requirements to file a Suspicious Activity Report on the matter.

4. *Consider Contacting SEC or SROs*. The firm should also consider whether to bring a data breach to the attention of the SEC or, if the firm is a broker-dealer, its primary SRO, including by informing the regulator of how the firm has responded to the breach, actions the firm has taken to mitigate further risk, and that the firm will furnish the regulator with a copy of the customer notification.

5. *Assess Customer Notification Obligations*. The firm should, of course, assess the extent to which it is obligated to notify customers, including under state laws that require notification of data breaches to customers.

6. *Carefully Draft Customer Notification.* The firm should prepare a form of notification. The notification should address the essential facts about the data breach, including as required by any applicable law, and information about the firm's response, including as applicable:

   - A general description of the incident, including the type of information breached;
   - The steps taken or to be taken by the firm, including to mitigate risk of further data breaches (*e.g.,* change of account credentials);
   - How customers may obtain additional information;
   - A reminder that customers should monitor their accounts and be attentive of their credit reporting history, if applicable; and
   - If the breach involves information that may potentially be misused to steal a customer's identify, an offer to provide customers with their credit reports for a period of time following the breach.
   - The information in the notification should be presented in a clear and conspicuous manner, not buried in other information given to affected customers.[19]

7. *Develop a Distribution Plan.* The firm should develop a plan for delivering the customer notifications by a means that the firm reasonably believes will enable the customer to receive the notification and that satisfies any applicable legal requirements. For example, if the customer has agreed to electronic delivery of notices, then it may be reasonable for the firm to provide data breach notification via e-mail.[20]

8. *Inform and Educate Your Client Service Representatives*. The firm should alert its client service representatives to the matter and the forthcoming customer notification and provide them with background in-

formation–such as a "questions and answers" document–so they are in a position to respond accurately to customer questions about the notification.

9. *Develop Press/Media "Talking Points."* Customer notification of data breaches tends to surface in the press. As such, a firm may want to consider preparing a press kit or "talking points," including essential information relating to the type of information breached the firm's response to the breach, and how the firm notified customers.

10. *Assess Insurance Needs*. Finally, a firm should review its insurance coverage and limitations as part of developing a plan for responding to data breaches. In some instances, a firm may inadvertently limit or exclude its insurance coverage due to its actions following a data breach. For example, some policies may exclude coverage if the insured fails to provide timely notice, admits wrongdoing without the insurance company's consent, or if the insured attempts to settle a claim without prior consent from the insurance company.

Conclusion

Adequately protecting personal information is an issue that securities and investment management firms should consider given the frequency with which data breaches are occurring. In fact, many firms may eventually experience a data breach. However, by taking a proactive approach, firms will be prepared to respond promptly to data breaches and possibly mitigate further damages.

Notes

1. Others have made this same observation in the broader context of financial services. *See* Wayne C. Matus, *Security Breaches: Are You Prepared For Litigation and a Consent Order?,* Electronic Banking Law and Commerce Report (January/February 2006) ("It seems as if, over the past two years, hardly a week has gone by without a news story revealing yet another security breach at yet another large financial institution or major business enterprise."); *see also* Lynne B. Barr and Jacqueline Klosek, Recent Developments in Data Security Law in the United States, Privacy & Data Protection (2006).
2. *See* Adel Melek and Marc MacKinnon, Deloitte Touche Tohmatsu, *2006 Global Security Survey*, 26 (June 2006). The final sample of firms represented in the survey consist of 31% of the top 100 global financial institutions, 34% of the top 100 global banks, and 16% of the top 50 global insurance companies.
3. *See* Privacy Rights Clearinghouse, *A Chronology of Data Breaches Reported Since the ChoicePoint Incident* (Updated October 31, 2006), *available at* <http://www.privacyrights.org/ar/ChronDataBreaches.htm> (reporting that there have been 256 data breaches so far this year and that the affected records from data breaches totals 95,668,529).
4. *See Data Breach Hype Is Misleading Consumers – Study,* Finextra (September 14, 2006) (reporting on a Javelin Strategy and Research study concluding that data breaches were responsible for only six per cent of all known cases of identity fraud).
5. *See* Ellen Nakashima, *Hackers Zero In on Online Stock Accounts*, Washington Post (October 24, 2006).
6. Ariz. Rev. Stat. § 44-7501 (2006); Ark. Code § 4-110 (2005); §§ 1798,29, 1798,82, and 1798,84 (2003); Cal. Civ. Code § 1798.29 (2002); Col. Rev. Stat. 6-1 (2006); 2005 Conn. Act 05-148 (Reg. Sess.); Del. Code Ann. tit. 6, §§ 12B-101-104 (2005); Fla. Stat. ch. 817.5681 (2005); Ga. Code §§ 910-912 (2005); Haw. Rev. Stat. § 481B (2006); Idaho Code §§ 28-51-104 through 28-51-107 (2006); 815 Ill. Comp. Stat. 530 (2005); Ind. Code § 24-4.9 (2006); 2006 Kan. Sess. Laws 196; La. Rev. Stat. §§ 3071-3077 (2005); Me. Rev. Stat. tit. 10, §§ 1346-1349 (2005); Minn. Stat. § 325E.61 (2005); Mont. Code Ann. §§ 1701-1722 (2005); Neb. Rev. Stat. § 9-705 through 9-707 (2006); N.H. Rev. Stat. Ann. § 359-19 (2006); Nev. Rev. Stat. §§ 205.461-205.4675 (2005); N.J. Stat. §§ 56:8-161 through 56:8-163 (2005); N.Y. Gen. Bus. Law § 208 (2005); N.C. Gen. Stat. §§ 60-66 (2005); N.D. Cent. Code § 51-30 (2005); Ohio Rev. Code § 1349.19 (2005); Okla. Stat. tit. 74, § 3113.1 (2006); 2005 Pa. Laws 94-2005; R.I. Gen. Laws §§ 11.49.2.1 through 11.49.2.7 (2006); Tenn. Code Ann. §§ 47.18.2101 through 2107 (2005); Tex. Bus. & Com. Code Ann. §§ 48.101-48.103 and 48.201-48.203 (2005); Utah Code Ann. §§ 13-42-101 through 13-42-301 (2006); VT. Stat. Ann. tit. 9, §§ 2430-2445 (2006); Wash. Rev. Code § 255.010 (2005); Wis. Stat. § 895.507 (2006). *See also*, New York City Intro. Nos. 139-A, 140-A, 141-A (2005).
7. *See, e.g.,* Ind. Code § 24-4.9-3(1)(a)(2) (2006); N.H. Rev. Stat. Ann. § 359-19.II (2006); N.Y. Gen. Bus. Law § 208(1)(a) (2005); 2005 Pa. Laws 94-2005(3)(b); R.I. Gen. Laws § 11-49.2-3(a) (2006).
8. Ariz. Rev. Stat. § 44-7501(G) (2006); Ark. Code § 4-110-105(d) (2005); Col. Rev. Stat. § 6-1-716(2)(a) (2006); Conn. Act 05-148(3)(b) (Reg. Sess.); Del. Code Ann. tit. 6, § 12B-102(a) (2005); Fla. Stat. ch. 817.5681(10)(a) (2005); Idaho Code § 28-51-105(1) (2006); 2006 Kan. Sess. Laws 196(3)(h); La. Rev. Stat. § 3074(G) (2005); Neb. Rev. Stat. § 9-705 through 9-707(3)(1) (2006); N.H. Rev. Stat. Ann. § 359-20.I(a) (2006); N.J. Stat. § 56:8-162(12)(a) (2005); Ohio Rev. Code § 1349.19(B)(1) (2005); Pa. Laws 94-2005; R.I. Gen. Laws §§ 11.49.2.3(a) (2006); Utah Code Ann. § 13-42-202(1)(a) (2006);Wash. Rev. Code § 19.255.010(10)(d) (2005).
9. *See* the Financial Data Protection Act, H.R. 3997, 109th Cong. (2005), the Data Accountability and Trust Act, H.R. 4127, 109th Cong. (2005), the Notification of Risk to Personal Data Act, S. 1326, 109th Cong. (2005), the Identity Theft Protection Act, S. 1408, 109th Cong. (2005), the Personal Data Privacy and Security Act , S. 1789, 109th Cong. (2005), the Cybersecurity Enhancement and Consumer Data Protection Act of 2006, H.R. 5318, 109th Cong. (2006), the Federal Agency Data Breach Notification Act, H.R. 5838, 109th Cong. (2006).
10. The SIA supports a uniform law to simplify the notification process for firms and clarify the requirements for consumers. *See* Testimony of Ira D. Hammerman, Senior Vice President and General Counsel, Securities Industry Association Securities Industry Association Before the Senate Committee on Banking, Housing and Urban Affairs (Sep. 22, 2005), *available at* <http://www.sia.com/testimony/2005/hammerman09-22-05.html>.
11. Section 630(k)(3) of the Financial Data Protection Act, H.R. 3997, 109th Cong. (2005) defines a "consumer reporter" as reporting agencies, financial institutions, or persons regularly responsible for compiling information for third parties, to provide or collect payment, to market products and services or for employment purposes using any means or facility of interstate commerce.
12. *See* the Financial Data Protection Act, H.R. 3997, 109th Cong. (2005).
13. *See* the Cybersecurity Enhancement and Consumer Data Protection Act of 2006, H.R. 5318, 109th Cong. (2006).

14. *See* Office of the Comptroller of the Currency, Treasury, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of Thrift Supervision, Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 59 (March 29, 2005) *available at* <http://www.occ.treas.gov/fr/fedregister/70fr15736.pdf>.
15. *See* Sara Hansard, *SEC Scrutinizes Firms for Vulnerability to Hackers,* Investment News (June 26, 2006). *See also* John H. Walsh, Associate Director, Office of Compliance Inspections and Examinations, U.S. Securities and Exchange Commission, Remarks at NRS 21st Annual Fall Compliance Conference (Oct. 5, 2006) (addressing identity theft concerns, providing suggestions for broker-dealers, investment companies and investment advisers when considering compliance programs relating to data protection, and indicating the impending release of a public report containing information from federal financial and other regulators and law enforcement agencies relating to identity theft).
16. *See* Dan Jamieson, *Theft at NASD Spurs Data Concerns,* Investment News (July 6, 2006).
17. *See* NASD, Notice to Members 05-49, Safeguarding Confidential Customer Information (July 2005) and NYSE, Information Memo 05-49, NYSE Rule 351(d)–Reports of Customer Complaint Statistics (July 21, 2005).
18. 17 C.F.R. §248.3(t) defines "nonpublic personal information" as "personally identifiable financial information," including "any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information that is not publicly available information, such as account numbers." The FFEIC guidance defines "sensitive information" as a customer's name, address or telephone number in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or personal identification number or a password to the customer's account.
19. A clear and conspicuous notice to customers may entail a communication dedicated solely for the purpose of informing the customer of the data breach as opposed to imbedding the notice within a correspondence regarding a different matter. 17 C.F.R. §248.3(c)(1) defines "clear and conspicuous" as "reasonably understandable and designed to call attention to the nature and significance of the information in the notice."
20. Although the SEC has made clear that broker-dealers, investment advisers and investment companies may use electronic media such as e-mail to deliver communications required to be delivered under the federal securities laws subject to certain requirements including customer consent, use of electronic media may be subject to other requirements under applicable state law or the Electronic Signatures in Global and National Commerce Act ("E-SIGN"), including the manner of obtaining or confirming customer consent to electronic communications. *See* 1995, 1996 & 2000 SEC releases (permitting oral, written and electronic consents); E-SIGN § 101(c)(1)(C)(ii), codified at 15 U.S.C. § 7001(c)(1)(C)(ii) (requiring that non-electronic consents be confirmed in a way that "reasonably demonstrates" access to the electronic disclosures).