Bloomberg BNA

Corporate Law & Accountability Report™

DATA SECURITY

Data Security: Looking for a Safe Harbor in a Gathering Storm



BY ROBERT KRISS, LEI SHEN AND REBECCA KLEIN

Robert Kriss is a partner in Mayer Brown's Privacy & Security group. Based in Chicago, he has represented suppliers and customers in IT outsourcing and software development disputes, has advised clients in the development of data protection and data breach response plans and has defended companies in data breach class actions. Bob holds Martindale Hubbell's highest A/V rating (AV Preeminent®) and has been recognised by Martindale Hubbell as among the ''Top Rated Lawyers of Technology Law.'' He also has served as an Adjunct Professor of Law at Northwestern University Law School, teaching trial advocacy.

Lei Shen is a senior associate in the Privacy & Security practice group in Mayer Brown's Chicago office. Lei focuses her practice on privacy and security, technology and business process outsourcing, and information technology transactions. Lei regularly advises clients regarding privacy, security, data transfer, data breach notification, telematics, and e-commerce issues.

Rebecca Klein is an associate in Mayer Brown's Privacy & Security group in the firm's Chicago office.

Introduction

In the past, regulatory enforcement in response to data breaches was limited, and most private class action litigation was dismissed for failure to allege the type of injury necessary to support standing to sue. As a result, companies that suffered data breaches rarely had to litigate the issue of whether they took reasonable steps to protect sensitive data before the breach occurred. Recently, a number of courts have rejected threshold legal defenses, such as standing, and are requiring companies to address the reasonableness of their actions before the breach. Whether these cases will be upheld on appeal and whether other trial courts will follow these precedents remain to be seen, but these decisions have changed the current risk profile of data breach litigation and have focused greater attention on the importance of implementing a reasonable data protection plan, both to prevent a data breach and to effectively defend against regulatory actions and litigation if a breach occurs.

Some experts in the field warn that even if reasonable measures are taken to protect data, a breach may still occur. Other experts claim that most breaches have occurred because reasonable measures were not taken. This debate is difficult to resolve because the causes of data breaches are rarely discussed publicly in much detail. Furthermore, the answer to the threshold question remains elusive: What are ''reasonable'' measures to take to prevent a data breach? If there was clarity as to what measures were reasonable and sufficient to avoid

 ISSN 2330-6300

the risk of liability and damage to business reputation, many companies would likely implement those measures.

Although it is not yet possible to find a completely safe harbor against liability arising from data breaches, it is possible to install dock bumpers and break waters to mitigate the risks created by the gathering storm. This article will review several important recent decisions that have changed the risk profile of data breach litigation and then offer a number of practical suggestions for mitigating those risks.

I. Four Recent Decisions Affecting the Risk Profile of Data Breach Litigation

Four recent decisions have heightened the liability risks associated with data breaches. The significance of each case is summarized below.

The Federal Trade Commission (''FTC'') has taken the position that it is authorized under the ''unfair practices'' provision of the FTC Act to bring enforcement actions against companies that suffer data breaches when the commission believes the companies failed to take reasonable steps to prevent the breach. The FTC contends that it is not required to specify through rulemaking what constitutes reasonable steps. Instead, the FTC argues that a general reasonableness standard analogous to the concept of general common law negligence, and further defined by industry standards and customary practices, is sufficient to satisfy the requirements of the statute and due process. In *FTC v. Wyndham Worldwide Corp*., 10 F. Supp. 3d 602 (D.N.J. 2014), the district court agreed with the FTC. The defendant has appealed the decision.

This decision raises the specter of companies having to prove after a breach occurs that they took reasonable steps to prevent the breach. Such cases would likely involve a battle of experts testifying based upon their view of reasonableness, presumably supported by their different views as to what constituted industry standards and whether compliance with industry standards was sufficient to satisfy the standard of reasonableness under the circumstances.

The court in *In re Adobe Systems Privacy Litigation*, No. 5:13-CV-05226-LHK, __ F. Supp. 2d __-, 2014 BL 252019 (N.D. Cal. Sept. 4, 2014) denied a motion to dismiss a misrepresentation claim on standing grounds. The plaintiffs' claims were based upon allegations that some, but not all, members of the putative class had suffered identify theft as a result of the data breach. The district court reasoned that the requirement that the risk of injury be ''certainly impending'' was met because the instances of identity theft that already had occurred were sufficient to establish that the risk of identity theft with respect to all members of the putative class had increased. Prior to this decision, most courts had found that putative class members who had not suffered identity theft but were, nonetheless, alleging an increased risk of identity theft lacked standing to sue.

This decision could open the door to significant damages claims to recover costs incurred by class members to prevent identity theft, such as the costs of subscribing to identity loss and credit monitoring services. Also, when a case is allowed to proceed beyond the motion to dismiss stage, the defendant will be required to respond to discovery requests that may be burdensome and intrusive, including requests to release sensitive information concerning the breach and the company's data protection systems to the plaintiff. Even if the discovery is subject to protective order, the company will have a limited ability to police compliance with the order. In addition, if the case were to proceed to trial, it is uncertain the extent to which the court would seal the courtroom when sensitive data security matters were addressed.

The significance of a company's posted privacy policy was highlighted in *In re LinkedIn User Privacy Litigation*, No. 5:12-CV-03088-EJD, 2014 BL 88977 (N.D. Cal. Mar. 28, 2014). In that case, the plaintiff alleged that the defendant made strong representations regarding data security in its publicly posted privacy policy and that these representations induced him to do business with the defendant. The privacy policy contained a statement that ''[a]ll information that you provide will be protected with industry standard protocols and technology.'' *Id.* at *1. The court denied a motion to dismiss for lack of standing. This case highlights the importance of being careful in representing the nature, extent and effectiveness of the company's data security policies and systems.

Finally, in *In re Target Corp. Customer Data Sec. Breach Litigation*, MDL No. 14-2522 (PAM/JJK), —__ F. Supp. 3d __, 2014 BL 338425 (D. Minn. Dec. 2, 2014), the court denied Target's motion to dismiss claims made by banks to recover losses arising from the theft of credit card information from Target. The court allowed a number of claims, including negligence, to go forward.

II. Risk Mitigation

The cases discussed above suggest that there is a meaningful risk that a company suffering from a data breach will become the target of regulatory or private class action litigation and will be required to demonstrate that it took reasonable steps to prevent the breach. To address this risk, a company should consider preparing and implementing a written information security plan (''WISP''), or if the company already has such a plan, should consider reassessing the plan to be current with recent threats and counter-measures. In addition, certain states, such as Massachusetts and Florida, either require companies doing business in those states to prepare and implement a WISP or submit one to the state in connection with a data breach, and companies in the financial service and health care industries also are required to prepare and implement such plans under the Gramm-Leach-Biley Act (''GLBA'') (15 U.S.C. 6801; 16 C.F.R. 314.3(a)) and the HITECH Act (45 C.F.R. 164.308; 45 C.F.R. 164.316), respectively.

An effective process for preparing a WISP will involve a collaboration of legal counsel, IT security specialists and a company representative/sponsor for the project. The WISP is not only an important tool for preventing data breaches and associated business losses; it also must be viewed as possibly the most important evidence in defending the company against regulatory enforcement actions and class actions if a data breach should occur. Because the plan and the process for preparing the plan may become evidence in a legal proceeding, it is important that the plan be prepared with legal input, including from lawyers who have experience handling evidence and trying cases.

  CARE ISSN 2330-6300

Legal counsel should be responsible for identifying any aspects of the plan that are required by law in light of the industry or geographic territory in which the company operates. For example, companies doing business in Massachusetts must encrypt the sensitive personal information of customers and employees when that information is transmitted over public networks or wirelessly, or stored on portable devices. *See* 201 MASS. CODE REGS. § 17.04. Similarly, Nevada requires that data collectors doing business in the state encrypt all personal information that is either transferred electronically outside of the secure system of the business or moved on any data storage device beyond the ''logical or physical controls'' of the data collector. NEV. REV. STAT. § 603A.215(2)(a)-(b). Another example of actions required by law is that financial service companies subject to the GLBA are required to name the board of directors as the primary body responsible for information security and the company is required to engage in regular testing of systems.

In addition, legal counsel should brief the other participants in the project as to what type of written record to create in developing the plan so that the effort will produce evidence that will be effective in a litigation context. Also, counsel's involvement in the process will increase the likelihood that aspects of the analysis and communications with experts may be kept confidential, subject to the attorney-client privilege. Such communications involving third-party data security specialists may be privileged to the extent that the analysis and communications are necessary for counsel to advise the client concerning what actions should be taken to comply with legal obligations. See, e.g., *United States v. Kovel*, 296 F.2d 918 (2d Cir. 1961).

Legal counsel also can offer advice as to the standards to use in performing the risk analysis and deciding what preventive measures to implement. One effective approach is to first perform a comprehensive mapping of the IT system to understand where sensitive data resides. Once the data is located, then an analysis of what protective measures should be implemented can be undertaken using standards that will be credible to a regulator, court or jury.

One such set of standards is the Payment Card Industry Data Security Standard (''PCI DSS''), which is applicable to companies involved in collecting and processing credit card information. The conceptual applicability of these standards is not limited to credit card information. The advantage of using these standards is that several states have recognized their usefulness by requiring companies involved in collecting and processing credit card information to be certified as compliant with these standards. For example, a Washington state statute provides that companies selling goods and services to Washington residents are not liable to financial institutions for reimbursement of costs relating to the reissuance of credit cards and debit cards arising from a data breach that affects account information if the company was in compliance with the PCI DSS. *See* WASH. REV. CODE § 19.255.020. Similarly, in Nevada, data collectors doing business in the state and accepting credit or debit card payments must comply with the PCI DSS and will not be liable for damages due to security breaches as long as they are in compliance with PCI DSS and the breach was not caused by gross negligence or intentional misconduct of the data collector. *See* NEV. REV. STAT. § 603A.215(1), (3). In addition, companies handling credit card information are usually contractually obligated to comply with these standards.

Although there may not be a consensus that PCI DSS is a sufficient standard to use in developing a WISP in all cases, the fact that both responsible governmental bodies and private parties attempting to prevent significant financial losses have decided that these standards are a reasonable tool to protect data should give these standards a high degree of credibility with regulators, judges and juries. No other set of data protection standards has received such a ''stamp of approval.''

Furthermore, even if compliance with PCI DSS might not be sufficient to avoid liability in every case, failure to comply with these standards could substantially increase the risk of liability. A regulator or private plaintiff could argue in court that the standards represent reasonable practices, and unless there is a good reason that the defendant did not have protective systems in place consistent with the standards, the defendant was negligent and should be held liable for losses suffered by third parties.

In summary then, companies should consider taking the following steps to mitigate the risk of liability arising from data breaches:

- Form a team consisting of a company representative/sponsor, legal counsel and third-party IT security specialist.

- The engagement letter for the security specialist should indicate that the specialist is being retained to assist legal counsel in providing advice to the company regarding its obligations to protect sensitive data.

- Legal counsel should brief the team on the process for developing the WISP and the type of documentation that should be created.

- The security specialist and company representative should be responsible for mapping sensitive information (such as social security numbers, health information, trade secrets, encryption keys) within the company's IT system.

- The team should decide what set of standards to use as the framework for the risk assessment and implementation of protective measures.

- The security specialist and the company representative should use the standards as a checklist to select protective measures to include in the plan. A list of practices/systems that the standards address but that are not implemented at the company should be compiled without characterizing them as necessary or as ''gaps.''

- The team, including legal counsel, should go through the list of potential practices/systems and make decisions as to what measures should be implemented. Reasons for the choices should be documented as part of the planning process.

- The plan should be drafted by the company representative and the security specialist and reviewed by legal counsel.

- The team should follow through and implement the plan after it is approved by management.

- The team should develop and conduct tests to determine whether the system provides adequate protection against internal and external threats.

■ Industry and government sources that can provide information about recent threats and countermeasures should be identified by the team and a process should be developed for the company to remain current on these subjects.

■ The plan should be reassessed if the company suffers a data breach to determine whether additional protective measures are necessary.

With regard to a board's involvement in the process:

■ The plan should be reviewed, revised if necessary and approved by the company's audit committee. Legal counsel and the security specialist should be available at the audit committee meetings to highlight key points and answer questions.

■ The audit committee should receive at least quarterly reports from the chief security officer regarding changes in the plan, test results and any data breach incidents.

■ At least once a year, the audit committee should have available an independent security specialist and outside counsel to answer any questions the audit committee may have concerning the adequacy of the company's data security systems and practices.

■ These suggestions are drawn from a recent decision in which the court dismissed stockholder derivative claims against board members. See *Palkon v. Holmes*, No. 2:14-CV-01234 (SRC), 2014 BL 293980 (D.N.J. Oct. 20, 2014) (holding that the board was protected by the business judgment rule against a shareholder claim where the board met numerous times to review breach issues, hired consultants and implemented recommendations).

Conclusion

In testimony before the Senate Commerce Committee on Mar. 26, 2014, Edith Ramirez, the chairwoman of the FTC, stated: ''The [FTC] has made it clear that [the law] does not require perfect security, and the fact that a breach occurred does not mean that a company has broken the law.'' However, FTC actions and recent court decisions suggest that companies should be prepared to prove that they took reasonable steps to protect data if a breach occurs. Establishing a well-organized and disciplined process, with appropriate legal input, to develop, implement and test a data protection plan is the best way to find a reasonably safe harbor in the gathering storm.

  CARE ISSN 2330-6300