Featured Article

The New Age of Data Security Breaches: A Practical Look at Corporate Exposure and Ways to Minimize Risk

Contributed by:
Cheryl A. Krause and Sarah Wager, Dechert LLP

As quickly as a credit card number can zip through cyberspace, a company's future and reputation can suddenly hinge on its liability for a data security breach. Earlier this year, for example, a Maine based supermarket chain, Hannaford Bros., announced that a data security breach exposed 4.2 million customer credit and debit card numbers, and at least 1,800 were stolen. Dozens of class action lawsuits were filed in a matter of days, seeking compensation for the breach and millions of dollars in damages. Lending Tree also was recently hit with multiple class action lawsuits after a data security breach in which company employees allowed mortgage lenders access to customers' confidential information on loan request forms. And just last month, after a class action lawsuit was filed against Ameritrade based on the plaintiffs' receipt of spam e-mails, a public citizen successfully opposed the preliminary class settlement, claiming Ameritrade failed to disclose the extent of the alleged breach or to take any corrective measures to protect its accountholders' private information.

Data falling into the wrong hands is certainly not a phenomenon unique to the Information Age, but the volume and scope of data security breaches involving electronically stored information, coupled with the massive press coverage many receive, has meant a world of hurt and worry for many companies. Catastrophic breaches can happen to any company that receives and stores personal information—which means virtually any company. Indeed, over 245 million records containing sensitive personal information have been subject to data security breaches in the United States since just January 2005.[1] And when a breach occurs, litigation is quick to follow.

Most companies know they need to adequately protect personal information to decrease the risk of a data security breach, and have a plan of action in case one occurs. However, a great many companies have failed to implement adequate information security policies, and have not developed a plan of action in case a security breach occurs. Many companies have already implemented such measures. In addition, the thorny tangle of state laws and a lack of a unifying federal law means even the best-intentioned companies find themselves aiming at a moving target. This article discusses core issues that companies should focus on to prevent, prepare for, and manage a data security breach amidst this constantly evolving area of law. It also highlights the potential litigation exposure stemming from a data security breach and ways to minimize that exposure.

Step One: Know the Company's Legal Obligations to Protect Personal Information and to Disclose Data Security Breaches

There is currently no comprehensive national law governing data protection or security breaches, although several such bills have been presented to Congress. There are a handful of federal and state statutes that specifically require a company to implement reasonable measures to secure "personal information"[2] and ensure the safe destruction of such data.[3] The current legal landscape has all the trappings of a compliance nightmare: forty-four states, the District of Columbia and Puerto Rico have enacted laws requiring notification to affected consumers and/or state agencies in the case of security breaches.[4] The federal government has layered on top of those statutes its own industry-specific laws governing, for example, the healthcare and financial services sectors.[5] The few states that have yet to move on the issue are likely to enact their own laws soon.

The states that have enacted breach notification laws have varying definitions of what constitutes "personal information," what triggers breach notification, and notification requirements. Each of these elements is crucial to the analysis of whether a breach occurred and if notification is required.

The statutory definition of "personal information" varies amongst the states, but most include an individual's first name or initial and last name combined with a: (1) social security number; (2) driver's license number or state issued identification card number; or (3) bank account, credit or debit card number with any required security code, or personal identification number that would permit access to an account. Some states have expanded this definition to include information such as medical information, passport numbers, employee identification numbers, unique biometric data, the date of birth, the mother's maiden name, and a digital signature.[6]

These statutes also lack uniformity in terms of who must comply with them. Broad state statutes require all persons, businesses and agencies that own or license personal information to disclose security breaches. Others have narrower application, such as applying only to "information brokers," which generally includes any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties. It generally does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes.[7]

Given this complex web of existing and developing law, it is important for companies to determine what types of sensitive personal information they obtain, and the existence and substance of applicable state and industry-specific data

protection and security breach notification laws, and to have in place a plan that is compliant with the broadest law on each issue.

Step Two: Have and Enforce Written Policies On The Protection And Destruction Of Personal Data And Management Of A Security Breach

The next key to compliance is to have written company policies on the subjects of data protection, document retention and destruction, and managing a security breach. The policies should be written in collaboration with the company's legal counsel, management, and IT department. However, as many companies have learned the hard way, once litigation has been initiated having a written plan is not enough. To support a defense against a lawsuit, these policies must have been implemented and enforced on a company-wide basis, as well as with any vendors or other corporate outsiders with access to the information.

A company's document retention and destruction policy (whether adopted as a separate policy or incorporated into a data protection policy) should categorize the personal information received by subject matter such as the type and sensitivity of data stored, and how the data is maintained, such as on paper or electronically. The policy should restrict access to sensitive or personal data, limit where the data can be stored (e.g., precluding storage on laptops), and establish communication protocols that can mitigate the risk of a security breach (e.g., requiring that all personal data be transmitted or formed in an encrypted format). The policy should also provide specific guidelines for retaining and destroying the different categories of data, including how long the data must be stored, when it must be destroyed, and how it must be destroyed.

The data protection and security breach policy should be framed by any industry-specific and state laws applicable to the company, any contractual obligations, and business realities. Critical to the analysis (and often overlooked) is consideration of applicable contractual obligations relating to data security, because such obligations often are more restrictive than the limitations provided by statute. To err on the side of caution, it is best to secure any type of personally identifiable information that can be used to facilitate identity theft or otherwise be misused. The company should carefully examine and periodically audit and update what personal information it stores and for how long. If unnecessary data is being requested and stored, the company should consider narrowing the information it requests from its customers or the categories of customers required to provide data.

Most security breach notification laws do not require notification if the affected personal information was encrypted. Accordingly, the company should conduct a cost-benefit analysis concerning data storage, destruction, and encryption. Other measures a company can implement to secure personal data include installation of firewalls and anti-virus software, restricted and monitored access to data such as password protection, and updating the system with the most current and best technology available.

Employees that have access to personal information should be trained on the company's document retention and data protection/security breach policies. The company should also consider creating and displaying notices about any potential criminal liability and other ramifications (such as termination) in the event an employee breaches the company's security policies.

Any policies the company adopts should regularly be reviewed and if necessary, revised, to comply with new legal obligations, and tested to ensure effectiveness and corporate compliance. A policy that exists but is not followed, or does not take into account the company's legal or contractual obligations, will not provide a strong litigation defense.

Step Three: Effectively Managing A Data Security Breach

Data security breaches occur in several ways, including stolen or lost laptops or computers, creation of fraudulent accounts, compromised passwords, hacking, employee theft, and lost back-up tapes. In the event of a breach, the key is to move quickly and secure legal counsel well-versed in resolving data breaches. A company that has a solid data security breach plan will be ahead of the curve.

Companies must immediately ascertain the type of data hacked, lost or stolen, if that data includes personal information, and if so, whose personal information. It should also determine whether the compromised information was encrypted, and what other steps were taken to protect it. This process should involve legal counsel, management, and IT. Once the nature and scope of the breach has been analyzed it is easier to determine whether there was a statutorily defined security breach such that notification is required.

A company conducting multi-state or national business must comply with the breach notification laws of each state where any individual whose data was compromised resides, and any applicable industry-specific federal law. This is one reason why it is imperative to have a current and regularly updated data protection and breach notification policy. If the company conducts business internationally, those laws should be examined as well.

What triggers the duty to provide notification of a security breach varies amongst the states. Most state breach notification laws only apply to computerized data, while a handful cover personal information stored on any medium, including paper.[8] Under the majority of state laws a security breach occurs under the statute only if there is an unauthorized "acquisition" of unencrypted, computerized, personal information. In a minority of states, unauthorized "access" to the information is

enough to trigger the notice obligation.[9] There is a safe harbor for almost all state notice laws if the personal information was encrypted at the time of the breach. Even if personal information is acquired in a security breach, some states only require notification where there is a reasonable risk of identify theft or some other harm, the breach is material, or misuse of the information has occurred or is likely to occur.[10]

States also vary on who must be notified of the breach. All require notification to affected state residents. Several also require notice to federal consumer reporting agencies, or state agencies such as the Attorney General, typically if a numerical threshold is satisfied. The company should also consider those whom it is contractually obligated to notify, such as its insurance carriers. Where the data at issue was received from other companies that are vendors or customers, it typically will be necessary for the company to have prompt and regular disclosure and close coordination with those other companies, in order to have a unified strategy and to maintain the vendor and customer relationships.

Even though it is not required in most states, the company should consider notifying law enforcement. The benefits of involving law enforcement include its resources, investigative techniques and expertise. However, the downside includes loss of control of the investigation, business disruptions, and heightened publicity. While notice of the breach must typically be made in the most expedient manner possible without unreasonable delay (which in some states, means within 45 days of discovery of the breach), in all states notice may delayed at the request of law enforcement.

Most states do not dictate the exact content of the breach notice. A proper notice, however, should describe the details of the security breach such as what happened, when, and the type of information affected. The notice should also explain the actions the company is taking to assist affected individuals, and should provide an adequate and easy to implement protection against identity theft, such as free credit monitoring (one free credit report per year) and identity theft insurance. The notice should also provide information on how affected individuals can protect their information, such as placing fraud alerts on their credit cards, and provide referrals to outside organizations that can assist with identity theft prevention and occurrences. Providing this type of assistance may help maintain goodwill and deter the success of lawsuits.

The approved methods for delivering notice are fairly consistent throughout the states. A company may provide notice by letter and e-mail, (e-mail notice is permitted only if there is consent to receiving e-mail notice), and a minority of states permit telephonic notice if it made personally and not by automated means. All states permit substitute notice where the cost of individual notice would be high and the number of affected individuals is large. Substitute notice is likely to require clear and conspicuous posting of the notice of the security breach on the business's web site home page and publication or broadcast in news media.

Step Four: Be Mindful Of The Potential For Civil Litigation In The Event Of A Security Breach And Take Steps Up Front To Minimize The Impact

Once a data security breach is disclosed, be prepared for a fight. In the past few years, hundreds of individual and class action lawsuits have been filed throughout the United States as a result of such breaches. These cases typically assert violations of state and federal data privacy and breach notification laws and common law tort and contract claims. Investigations and actions also can be brought by the Federal Trade Commission and the State Attorneys General.

Private actions stemming from data security breaches are a fairly new occurrence, yet hundreds have been filed and have resulted in some identifiable trends. A private right of action cannot be maintained unless provided by law. Some state statutes permit a private right of action for violations of reasonable data security provisions and their breach notification statutes, while other states allow enforcement only by the Attorneys General.[11] If a private right of action is determined to exist, the plaintiff must have standing to bring suit. Courts have held that plaintiffs lack standing unless they have experienced an actual injury, but some have found that standing requires a low threshold in terms of the injury requirement, permitting actions to proceed if there is a possibly identifiable injury.[12] In examining whether there is sustainable injury to maintain a cause of action in the security breach context, courts are routinely finding that fear and apprehension of fraud, losing money and identity theft do not constitute a legally recognizable injury.[13] A mere increased risk of identity theft, the burden and cost associated with credit monitoring, closing compromised credit accounts and opening new accounts, and scrutinizing credit card statements are also not considered injuries.[14] Since the tort and contract claims that have been asserted in these cases require damages, the courts have dismissed such actions for failure to meet a required claim element. In cases whether there has been an identifiable injury such as identity theft or other financial crime, actions typically may proceed.

Additionally, these common law claims require a duty-imposing relationship or statutory duty to secure personal information for liability to attach. If the data security breach stems from theft outside the company, such as an in-home burglary where a company laptop storing personal information is stolen, courts have found the theft was not foreseeable and have declined to impose liability based on lack of causation.[15]

A company sued for breach of the data security and breach notification laws has several defenses such as: 1) that the company had no duty; 2) if a duty existed, that duty has been satisfied; 3) causation cannot be demonstrated; and 4) no injury has been demonstrated which is recoverable by law. If the company is defending a class action suit, it can also argue that the class action requirements have not been met, such as no commonality or typicality, that the plaintiff lacks standing, and that the class has inadequate representation.

Available defenses vary based upon the facts of the case and jurisdiction in which it is being litigated. Consulting with legal counsel immediately after the potential breach can assist with preserving any applicable defenses.

Although lawsuits not alleging actual identity theft or other financial crime have been largely unsuccessful, it is important to note that Minnesota has already enacted, and other states are considering, legislation making a company automatically liable if personal information is stored unnecessarily. Minnesota's new law, effective August 2008, prohibits merchants who do business in that state from storing personal information obtained from swiping credit cards for more than 48 hours.[16] If violated, a financial institution has standing to sue the company for reasonable costs associated with security breaches to protect cardholders.

New laws such as these – covering discreet areas of data protection and breach notification requirements – underscore the need for companies to keep up on the law and to update regularly their data retention, data security, and breach notification policies.

Cheryl A. Krause is a partner in the White Collar and Securities Litigation Group of Dechert LLP. She has defended numerous corporations and individuals in cybercrime and other white collar criminal and regulatory matters and has taught Cybercrime at University of Pennsylvania Law School. Ms. Krause is a former Assistant U.S. Attorney in the Southern District of New York and former clerk for the Honorable Anthony M. Kennedy of the United States Supreme Court. She is the recipient of numerous awards and has been named an "up and coming" lawyer for white collar litigation and government investigations by Chambers USA. Ms. Krause can be reached at (215) 994-2139 or at Chambers USA. Ms. Krause can be reached at (215) 994-2139 or at cheryl.krause@dechert.com.

Sarah Wager is an associate in the Intellectual Property Group at Dechert LLP. She focuses her practice on patent, trade secret, trademark, and unfair competition litigation, business torts, securities fraud matters, shareholder derivative suits, and class actions, providing her clients with business-focused strategies. She has experience handling matters before federal and state trial and appellate courts, as well as representing clients in alternative dispute resolution. Ms. Wager can be reached at (650) 813-4875 or at sarah.wager@dechert.com.

---

[1] *See* Privacy Rights Clearinghouse, "A Chronology of Data Breaches" (*available at* http://www.privacyrights.org/ar/ChronDataBreaches.htm) (last visited Oct. 6, 2008).

[2] *See, e.g.*, NRS 603A.210; Tex. Bus. & Com. Code § 48.102; R.I.G.L. § 11-49.2-2.

[3] *See, e.g.*, Cal. Civ. Code § 1798.81; NRS 603A.200; Tex. Bus. & Com. Code § 48.102.

[4] *See* National Conference of State Legislatures, "State Security Breach Laws" (*available at* http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm) (last visited Oct. 6, 2008).

[5] The federal sectors that have adopted data protection and security breach notification laws use industry-specific factors to determine what information must be protected. For example, the Gramm-Leach Bliley Act (GLBA) requires financial service providers to secure consumers' personal financial information, and the Health Insurance Portability and Accountability Act (HIPPA) restricts the disclosure of health information relating to individual physical or mental conditions, and the receipt and payment of care.

[6] *See, e.g.*, Cal. Civ. Code § 1798.82 (medical information and health insurance information); Neb. Rev. Stat. 87-802(5) (unique biometric data); N.D.C.C. § 51-30-01 2.a. (birth date, employee ID number, mother's maiden name, digital signature).

[7] *See, e.g.*, Ga. Code Ann. §§ 10-1-911 and 912 (applies to "information brokers"); 10 M.R.S.A. §1347 (applies to "information brokers"); Okla. Stat. tit. 74, § 3113.1 (applies "any state agency, board, commission or other unit or subdivision of state government that owns or licenses computerized data that includes personal information").

[8] *See, e.g.*, HRS § 487-2; I.C. § 24-4.9-2-2; N.C.G.S. § 75-65(a).

[9] *See, e.g.*, Conn. Gen. Stat. § 36a-701(b); 9 V.S.A. § 2430(8)(A).

[10] See, e.g., Fla. Stat. § 817.5681(4)(2005) ("materially compromises the security, confidentiality, or integrity of personal information"); N.C.G.S. § 75-61(14) ("illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer"); R.C. 1349.19(A)(1)(a) ("reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property").

[11] *See, e.g.*, A.R.S. § 44-7501; 6 Del. C. § 12B-104; R.C. 1349.192.

[12] *See, e.g.*, *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121 (N.D. Cal. Mar. 24, 2008) (denying motion for judgment on the pleadings as to negligence claim based on theft of laptop computers containing personal information of on-line applicants, finding that plaintiff presently has standing to assert a claim based on alleged harm of increased risk of identity theft because there is not enough information for the court to determine whether the risk is actual, imminent, or credible; also denying motion to strike class allegations as premature and redundant of the motion for judgment on the pleadings); *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, No. 07-CV-02480, (S.D.N.Y. Aug. 28, 2008) (granting motion for summary judgment as to breach of fiduciary duty and negligence claims based on theft of a laptop containing personal information because there was no evidence that the data was compromised and the laptop was password protected, but denying motion for summary judgment as to breach of contract claim based on need for additional discovery).

[13] *See, e.g.*, *Shafran v. Harley-Davidson, Inc.*, No. 07-CV-01365, (S.D.N.Y. Mar. 20, 2008) (dismissing class action complaint based on loss of computer with personal information because expense of credit monitoring to combat an increased risk of identity theft is not an injury); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 635-40 (7th Cir. 2007) (affirming district court's dismissal of class action complaint for negligence based on breach of on-line banking service application database, finding that the damages sought for expenses to prevent current and future use of personal information are not cognizable under Indiana law); *McCall v. Certegy Check Services, Inc.*, No. 07-CV-00578, (W.D. Mo. Dec. 12, 2007) (dismissing class action based on employee's theft and resale of personal information because the increased risk of identity theft is not an injury under the asserted common law claims); *Ponder v. Pfizer, Inc.*, 522 F. Supp. 2d 793 (M.D. La. 2007) (dismissing class action complaint based on unauthorized access and coping of employee personal information, finding that alleged "fear and apprehension of fraud, loss of money, and identity theft; the burden and cost of credit monitoring; the burden and cost of closing compromised credit

accounts and opening new accounts; the burden of scrutinizing credit card statements and other statements for unauthorized transactions; damage to [ ] credit; loss of privacy; and other economic damages" were speculative); *Hendricks v. DSW Shoe Warehouse, Inc.*, 444 F. Supp. 2d 775 (W.D. Mich. 2006) (dismissing class action breach of contact complaint seeking reimbursement for costs of credit monitoring products purchased by plaintiffs after DSW's computer network containing customer personal financial information was compromised by an unauthorized third party because plaintiff failed to allege damages that are recognizable under Michigan law); *Bell v. Acxiom Corp.*, No. 06-CV-00485, (E.D. Ark. Oct. 3, 2006) (motion to dismiss granted for lack of standing because Plaintiff's allegations that she suffered an increased risk of both receiving unsolicited mailing advertisements and of identity theft were speculative and receipt of unsolicited and unwanted mail does not constitute actual harm).

[14] *See, e.g.*, *Kahle v. Litton Loan Servicing, LP*, 486 F. Supp. 2d 705 (S.D. Ohio 2007) (summary judgment granted because customer did not suffer cognizable injury as result of theft because no unauthorized use of customer's personal information had occurred, customer waited until almost one year after theft to obtain credit monitoring and chose not to place free fraud alert on her credit report, and there was no evidence that information was target of the theft or that thieves were able to access her information).

[15] *See, e.g.*, *Guin v. Brazos Higher Educ. Serv. Corp.*, No. 05-CV-00668, (D. Minn. Feb. 7, 2006) (no causation for negligence claim based on because theft of laptop in home burglary was unforeseeable).

[16] *See* Minn. Stat. § 325E.64; *see also* S.B. 1675, 95th Gen. Assemb., Reg. Sess. (Ill. 2007); H.B. 3222, 80th Gen. Assemb., Reg. Sess. (Tex. 2007).