March 2014

Weil

Class Action Monitor

Anticipating the Inevitable: What Every Company Should Think About Before a Data Breach Occurs

By Christopher Cox, David Singh, John Stratford, and Jennifer Ramos

In This Issue

1 Anticipating the Inevitable: What Every Company Should Think About Before a Data Breach Occurs

5 An Overview of the Telephone Consumer Protection Act: Managing the Legal Risks

Introduction

Businesses today collect ever-increasing amounts of personal information about their customers, from account passwords and email addresses to highly sensitive medical and financial information. Well-funded, sophisticated hackers are always looking for ways to obtain such information or access and exploit a company's most sensitive, confidential data. As a result, companies face greater risks than ever from lapses in data security. The Privacy Rights Clearinghouse reported 602 data security breaches in the United States in 2013 alone, comprising over 55 million individual records.[1] These breaches have many causes, including criminal hacking, intentional leaks by insiders, unintended public disclosures, lost laptops or flash drives, and general negligence. As a result, data breaches are difficult to predict and even more difficult to prevent.

A data breach can result in massive exposure for businesses. According to a recent study, the average cost of a data breach to a U.S. company was $188 per record compromised.[2] If thousands or even millions of customer records are affected, the damages may be substantial – this is repeatedly evidenced as more and more well-known companies experience data breaches. In 2007, for example, the TJX Companies projected costs of over $250 million due to a data breach involving the theft of some 45 million customer credit and debit card numbers.[3] Target Corporation is still incurring costs from the late-2013 criminal hacking of its point-of-sale systems and the accessing of sensitive information belonging to millions of customers, including debit and credit card data.

The costs from a breach of data security are varied. In addition to the immediate expenses for investigating and repairing the breach, companies should expect to incur costs to notify affected parties, manage public relations, and respond to government inquiries and investigations. A company may also face legal action on multiple fronts, from consumer or shareholder class actions to lawsuits from affected business partners to FTC or state attorney general enforcement actions. And, perhaps most significantly, there may be a serious long-term reputational impact on the business's brand or customer relationships.

The likelihood of a data breach and the risks involved are so high that the possibility can no longer be ignored – companies must take the initiative to reduce the likelihood of a breach and to reduce the impact of a breach when the inevitable occurs. In addition, it is essential for affected businesses to retain counsel with expertise in rapidly evolving data privacy laws and the ability to effectively handle the onslaught of litigation in the aftermath of a data breach, including class actions and regulatory enforcement actions. Although there is no piece of comprehensive federal legislation dictating the nature of security practices companies must adopt, businesses should be aware of the numerous federal statements regarding data security, including Executive Orders,[4] White House policy directives,[5] FTC guidelines,[6] pending regulatory frameworks,[7] and proposed legislation[8] that could be argued to constitute a minimum standard of care. The imminent introduction of new data privacy directives in the European Union also means that companies doing business in Europe should consult counsel with international capabilities.

Below are suggested best practices for companies to follow to anticipate, prevent, and respond to a data breach.

Best Practices in Preparing for and Responding to a Data Breach

Before a Data Breach Occurs:

- *Anticipate* – Catalog all confidential data owned or maintained by the company and ensure that proper security procedures are in place for keeping it safe. Conduct ongoing risk assessments, invest in state-of-the-art security measures, and hire "ethical hackers" to test data security. It is important to understand that most companies are targeted for intrusion because of exploitable security weaknesses, not because of their high profiles or the value of their confidential information.[9] Testing the integrity of the system on a regular basis is a wise investment.
- *Train* – Inform employees and vendors of proper security procedures and periodically review and update data security policies.
- *Organize* – Create a response team to implement a plan of action when a breach occurs. The team should be multi-disciplinary and composed of senior management, IT, legal, and public relations personnel. The plan should include procedures for promptly identifying and repairing the breach, investigating the cause of a breach, analyzing the implications of the breach, and notifying the necessary parties.
- *Insure* – Consider purchasing cyber insurance. Carefully consider the scope of coverage and exclusions under a data breach policy, including whether the policy covers costs related to lawsuits, regulatory investigations, internal investigations, notifications to affected consumers, public relations management, credit monitoring, and/or statutory penalties. A recent study showed that less than a third of companies surveyed had procured data breach insurance, but that companies were increasingly considering this option.[10]

After a Data Breach Occurs:

In the aftermath of a data breach, a company may still be investigating the cause when notification is required by applicable state and federal statutes or when an attorney general investigation begins. As such, it is important for the organization to respond quickly and proactively by assembling its response team and implementing its plan as soon as it learns of the breach.

First, take the necessary steps to secure the system to prevent further data loss, isolate any malware, and repair the breach. The data breach response team should also investigate the cause of the breach, recommend and implement corrective action, and test the integrity of the restored or alternate system.

Next, work with counsel to analyze the legal and regulatory implications of the breach. This requires an understanding of what data has been compromised, whether the data was encrypted or otherwise made inaccessible, the risk that data will be used by third parties, who will be adversely affected, who should be notified and when (including whether notification may be delayed until the integrity of the system is restored), and whether insurance will cover costs related to the breach.

If necessary, work with outside counsel regarding potential obligations to contact law enforcement. While law enforcement or regulatory bodies may commence their own investigations, some state notification statutes require businesses to contact enforcement agencies or delay notification of consumers in the event of a breach.

Additionally, it will likely be necessary to notify the affected parties and implement a public relations plan to mitigate reputational harm. Because a company will likely be required by statute to notify customers or business partners affected by a data breach, an effective public relations plan should include model notice templates and scripts for relaying information about the incident and mitigation steps to the public in a consistent and timely manner. Companies may also consider notifying the public even if they are not legally required to do so in order to avoid subsequent negative publicity. Weil has relationships with vendors and extensive expertise that can help your company anticipate potential issues and formulate best practices for notifying individuals and the public.

Anticipate and prepare for inevitable litigation. A company adversely affected by a data breach may consider filing suit against those responsible for the breach; likewise, customers or business partners affected by the breach may decide to pursue civil remedies against the company or its executives. Securities and consumer class actions are likely, although this area of the law remains unsettled. The constitutional requirement of standing is just one example of the uncertainty in this area: some courts have found that consumers lack standing to sue unless they can show a concrete injury resulting from a data breach, while others have allowed consumer class action suits to go forward after a data breach even where no customer data was actually misused. In addition, state attorneys general may institute claims against companies even where individual and class actions might fail due to lack of standing to sue or failure to identify cognizable harms.

The aftermath of the breach may also include regulatory action. State and federal authorities may launch their own investigations into the causes of the breach, not only to prosecute criminals who may have caused the breach but also for consumer protection. Such investigations could include monetary penalties and required periodic audits lasting decades. The FTC in particular has used its authority under the FTC Act in recent years to assert that a company's failure to take adequate steps to protect consumer information constitutes an unfair trade practice under the Act. For example, after a security breach in 2005 involving 40 million credit card numbers, the FTC prosecuted CardSystems Solutions, Inc. and required it to adopt stricter security measures and conduct an independent audit every other year for the next twenty years. Companies subject to investigations need counsel to work with federal agencies, like the FTC, as well as state agencies in the immediate aftermath of a breach to facilitate investigations and limit potential penalties.

Whether a company will be bringing an action against data thieves or defending against consumer class actions, suits by business partners, or regulatory investigations, it is vital to diligently prepare for litigation and to choose counsel well-versed in data privacy issues.

Data Breach Notification Laws

When a data breach occurs, the law may require notification of affected parties or government agencies. Navigating the tangled web of notification statutes is a particular area of concern for companies recovering from a data breach. An assortment of state and federal notification laws may apply in any data breach situation; the following is a brief summary of the federal and state law trends in this area.

Federal Law

Despite pushes for a uniform body of federal laws governing cybersecurity threats and data breaches, there is currently no law providing a uniform set of rules governing data breach notification. Depending on the type of organization and the type of data involved, however, specialized federal laws may apply.

For example, the Gramm-Leach-Bliley Act requires financial institutions to notify customers of a breach, while SEC regulations and the Sarbanes-Oxley Act have been interpreted as imposing certain reporting obligations on publicly traded companies in the wake of a data breach. Other pertinent federal laws

relating to cybersecurity may include the FTC Act, the Health Insurance Portability and Accountability Act, the Health Information Technology for Economic and Clinical Health Act, the Controlling the Assault of Non-Solicited Pornography and Marketing Act, and the Children's Online Privacy Protection Act. Companies and counsel must be aware of their potential obligations under these and other federal laws.

State Law

To date, forty-six states have enacted statutes requiring some form of notification following a data breach. Most are patterned after California's notification statute and thus share many of the same requirements. Generally, the statutes require companies or state agencies to notify state residents in a timely fashion when the company or agency becomes aware of a loss of unencrypted data containing a state resident's personal information. They also provide an exemption from compliance with the statute where a company maintains its own breach notification policy and the policy is consistent with the requirements of the statute. Some states also call for notification of the state attorney general or consumer reporting agencies, depending on the extent of the breach. If a company fails to comply with the breach notification statute, it may be subject to civil penalties enforced by the attorney general; a minority of state statutes also provide for a private cause of action.

Despite these similarities, variations exist. Some states require consumer notification whenever a breach occurs, while others only require notification if an assessment determines that misuse of the information is likely. Some states permit companies to delay notification pending an investigation to assess the breach and restore the integrity of the data, while others require notification within a certain time period. Even states permitting companies to delay notification for the purposes of investigation have different timing requirements governing when a company must notify consumers after it concludes its investigation. While many states require notice to be provided "without unreasonable delay," other states are much stricter, with some states requiring notice to consumers within 45 days of a breach or requiring notification of the appropriate government agency within 10 days. In responding to a data breach situation, special care and expertise are required to analyze and comply with the patchwork of state laws in this area.

In the next month, Weil will publish a comprehensive analysis of each state's data breach statutes and reporting requirements. To request a copy, please email public.relations@weil.com with "Data Breach Survey Request" in the subject line.

---

1. *Chronology of Data Breaches*, Privacy Rights Clearinghouse (accessed Mar. 3, 2014), https://www.privacyrights.org/data-breach/new.
2. *See* Ponemon Institute, LLC, *2013 Cost of Data Breach Study: Global Analysis*.
3. *See* Ross Kerber, *Cost of Data Breach at TJX Soars to $256m*, Boston Globe, Aug. 15, 2007, http://www.boston.com/business/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/?page=full.
4. *See* Exec. Order No. 13636, 78 Fed. Reg. 11,737 (2013).
5. *See* White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012), available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf; White House, *Presidential Policy Directive – Critical Infrastructure Security and Resilience* (February 12, 2013), available at http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
6. *See generally* FTC, *Data Security*, http://business.ftc.gov/privacy-and-security/data-security; *see also FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012), available at http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
7. *See* National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
8. *See* Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (2014); Data Security Act of 2014, S. 1927, 113th Cong. (2014).
9. *See* Verizon, *2012 Data Breach Investigations Report* at 3.
10. *See* Ponemon Institute LLC, *Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age*, August 2013.

An Overview of the Telephone Consumer Protection Act: Managing the Legal Risks

By David Singh and Jessica Mohr

Congress enacted the Telephone Consumer Protection Act (TCPA) in 1991 because of consumer complaints regarding aggressive telemarketing techniques. *See, e.g. Mims v. Arrow Fin. Servs., LLC*, 132 S. Ct. 740, 742 (2012). Today, the TCPA extends far beyond the aggressive telemarketing of the early 1990s and governs a broad range of contact between companies and their customers by fax, text message, or prerecorded message. This article provides an overview of the broad range of advertising activities prohibited by the TCPA, as well as the legal risks.

The TCPA, codified in 47 U.S.C. § 227, provides that it is unlawful to make a call (other than for an emergency or with prior express consent) using an "automatic telephone dialing system or an artificial or prerecorded voice" to an emergency line, hospital room or similar facility, or a telephone number where the receiver is charged for the call, and also prohibits calls to residential telephones "using an artificial or prerecorded voice to deliver a message" absent an emergency or express consent. 47 U.S.C. § 227(b)(1)(A) and (B). Further, the TCPA prohibits unsolicited advertisements sent to fax machines and the use of "an automatic telephone dialing system" which engages two or more lines of a business. 47 U.S.C. § 227(b)(1)(C) and (D). Importantly, a text message fits the definition of a call for purposes of the TCPA. *See Satterfield v. Simon & Schuster, Inc.*, 569 F.3d 946, 952 (9th Cir. 2009).

The TCPA provides for damages of $500 for **each** infraction, which can be increased to $1500 for willful violations with no cap on the total damages amount. 47 U.S.C. § 227. Accordingly, where a company communicated with a large number of customers or potential customers, potential exposure under the TCPA can be immense. As a result, the TCPA has become a new favorite statute of the class action plaintiff's bar, which filed an unprecedented number of TCPA cases in 2013. Moreover, the recent wave of TCPA litigation has resulted in several high-profile settlement awards in the tens of millions of dollars.

TCPA cases often involve unauthorized calls from an automatic telephone dialing system (ATDS). Parties engaged in telemarketing practices should be particularly aware that a system must have certain characteristics to be considered an ATDS, but those characteristics do not have to be in use. *See Satterfield*, 569 F.3d at 951. In *Satterfield*, the Ninth Circuit held that a "system need not actually store, produce, or call randomly or sequentially generated telephone numbers, it need only have the capacity to do it." *Id*. The Ninth Circuit's ruling in *Satterfield* serves as a cautionary tale for any party engaged in telephonic advertisements – if the party's ATDS has the required capability and then makes an uninvited call to a consumer, the party may be subject to liability under the TCPA.

Another prevalent and related issue in TCPA cases is prior express consent. Prior to recent changes by the Federal Communications Commission (FCC), prior express consent to receive autodial telemarketing calls or text messages could be obtained if the party voluntarily provided her phone number, or through other implied conduct. *See Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CC Docket No. 92-90, Report and Order, 7 FCC Rcd. 8752, 8769 ¶ 31 (1992) ("Persons who knowingly release their phone numbers have in effect given their invitation or permission to be called at the number…").

The FCC's new interpretation of "prior express consent," effective October 21, 2013, now requires express written consent for the receipt of prerecorded messages and autodialed calls and/or text messages made to cell phones and prerecorded and autodialed calls made to residential land lines for the purposes of advertising. *See Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, 27 FCC Rcd. 1830, 1838-40 ¶¶ 20-26 (2012). This new interpretation makes it much more difficult to obtain the express consent of a consumer because it requires that the consumer receive a "clear and conspicuous disclosure" that they will receive future calls or messages, and consent cannot be a condition of their making a purchase. *Id*. at ¶ 32. Moreover, the FCC abolished the established business relationship

exception for prerecorded telemarketing calls to residential land lines. *Id*. at ¶¶ 35-43. Previously, if a person had made a purchase from a company, that company could engage in autodial advertising without the express written consent of the purchaser. *See, e.g., CE Design, Ltd. v. Prism Bus. Media, Inc.*, 606 F.3d 443, 451 (7th Cir. 2010). Now, however, express written consent is required.

Importantly, express written consent is only required if the autodial call or text is made for telemarketing purposes. Indeed, if the call or text is made for informational purposes, consent is still established if the consumer voluntarily provided her phone number. *See Baird v. Sabre, Inc.*, No. CV 13–999 SVW, 2014 WL 320205 (Jan. 28, 2014). In *Sabre*, the court found that by voluntarily providing a phone number while booking a flight, the consumer was consenting to be contacted at the phone number regarding her flight. Thus, companies using autodial technology should be aware of the distinction between telemarketing and calls or texts which simply provide information about a purchase.

Companies engaged in autodial advertising should also be aware that a consumer can revoke their prior express consent. The Third Circuit Court of Appeals, the first Court of Appeals to address the issue, held that a consumer can revoke her prior express consent despite the fact that 47 U.S.C. § 227 does not contain any express language granting consumers this right. *See Gager v. Dell Fin. Servs., LLC*, 727 F.3d 265, 270 (3d Cir. 2013). The Third Circuit concluded that the statutory silence on the issue of revocation should be construed in favor of consumers. *Id*.

Consent is an especially important issue in class actions, as the requirement of express consent may be used to defeat the "typicality" and "commonality" requirements under Federal Rule of Civil Procedure 23. *See* Fed. R. Civ. P. 23. For example, the Fifth Circuit denied class certification in a case related to consumers' receipt of junk fax advertisements because the issue of consent for each potential class member was individualized. *See Gene and Gene LLC v. BioPay LLC*, 541 F.3d 318, 329 (5th Cir. 2008). Similarly, the Seventh Circuit found that a class representative's claims were not "typical" of the claims of the rest of the class members because the representative's claims were potentially subject to the consent defense, and ordered the district court to reconsider the plaintiff as class representative. *See CE Design Ltd. v. King Architectural Metals, Inc.*, 637 F.3d 721 (7th Cir. 2011).

Companies using autodial advertising should consider procedures for obtaining express written consent, especially considering the FCC's new interpretation. Where applicable, express consent is an important defense which can help companies avoid liability and potentially immense monetary exposure. Indeed, in *CE Design*, the Seventh Circuit remarked on the potential amount of damages in discussing class certification where the defendant had "faxed some 500,000 ads" which the plaintiff contended did not fall within any exception, including prior express consent. *Id*. at 724. At $500 per infraction, 500,000 offending faxes could result in $250 million in damages. Given the magnitude of potential exposure under the TCPA, companies engaged in any type of autodial advertising should take notice of the new FCC regulations, and in particular the prior express consent issue, to ensure that they are compliant with the TCPA and not subject to liability thereunder.

Class Action Monitor is published by the Litigation Department of Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

If you have questions concerning the contents of this issue of *Class Action Monitor*, or would like more information about Weil's Class Action practice, please speak to your regular contact at Weil, or to the editors or authors listed below:

Editor:

David Singh (Silicon Valley)	Bio Page	david.singh@weil.com	+1 650 802 3010

Contributing Authors:

Christopher Cox (Silicon Valley)	Bio Page	chris.cox@weil.com	+1 650 802 3029
Jessica Mohr (Silicon Valley)	Bio Page	jessica.mohr@weil.com	+1 650 802 3012
Jennifer Ramos (NY)	Bio Page	jennifer.ramos@weil.com	+1 212 310 8280
David Singh (Silicon Valley)	Bio Page	david.singh@weil.com	+1 650 802 3010
John Stratford (Silicon Valley)	Bio Page	john.stratford@weil.com	+1 650 802 3122