MLRC Media Law Resource Center
BULLETIN
2015 Issue No. 1 May 20115

Legal Frontiers in Digital Media

TABLE OF CONTENTS

MEDIA LAW RESOURCE CENTER, INC.

520 Eighth Avenue, North Tower, 20 Floor, New York, NY 10018

medialaw@medialaw.org | www.medialaw.org | 212-337-0200

EMERGING THEMES IN DATA BREACH LITIGATION: WHAT IN-HOUSE COUNSEL NEED TO KNOW

By Jonathan H. Blavin and Jesse M. King

Jonathan H. Blavin is a partner at Munger, Tolles & Olson. His practice focuses on high-technology privacy and intellectual property disputes. Jesse M. King is an attorney at Munger, Tolles & Olson. His practice focuses on white collar investigations and technology.

It seems that almost every other day a new high profile data breach makes headlines. In December 2013, an attack exposed payment card data and personally identifiable information for millions of Target customers when hackers installed malware on point-of-sale terminals.[1] The breach cost Target at least $148 million in legal, consulting, and credit monitoring services.[2] Just months after the "unprecedented" Target breach, Home Depot revealed a data breach with an even larger exposure of credit card information.[3] Home Depot warned investors that the data breach had cost $43 million and resulted in dozens of lawsuits and a number of government investigations that could adversely affect the company's business operations.[4] Indeed, a recent study found that the number of disclosed data breach incidents had increased by 28.5% from 2013 to 2014, with a record 1.1 billion personal and sensitive records compromised in 2014.[5]

The increase in security incidents also has led to increased and improved data security practices. One survey of U.S. executives found that between 2013 and 2014 there was an over 70% increase in the percent of companies with a data breach response plan and data breach response team in place.[6] As industry awareness and coordination increases, companies can be better prepared to prevent or mitigate the consequences of security incidents.[7] In-house counsel can lead the way by taking practical steps to mitigate the risks under the evolving state of play in data breach law.

Although the nature of attacks and the laws governing companies affected by an attack are evolving every year, this article discusses five themes that in-house counsel should bear in mind as they develop internal policies and protocols: (1) breach notification requirements are largely governed by heterogeneous state laws, (2) security measures are often evaluated under a context-driven reasonableness standard, (3) plaintiffs may have difficulty in establishing a sufficient injury, (4) different types of data require different levels of protection, and (5) data breach insurance coverage is unsettled.

---

[1] Sara Germano, *Target's Data-Breach Timeline*, WALL STREET JOURNAL BLOGS: CORPORATE INTELLIGENCE (Dec. 27, 2013, 6:28 PM), http://blogs.wsj.com/corporate-intelligence/2013/12/27/targets-data-breach-timeline; Keith Jarvis & Jason Milletary, *Inside a Targeted Point-of-Sale Data Breach*, DELL SECUREWORKS (Jan. 24, 2014), http://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf.

[2] Rachel Abrams, *Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop*, N.Y. TIMES (Aug. 5, 2014), http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html.

[3] Jim Finkle & Nandita Bose, *Home Depot Breach Bigger Than Target at 56 Million Cards*, REUTERS, Sept. 18, 2014, *available at* http://www.nytimes.com/reuters/2014/09/18/business/18reuters-home-depot-dataprotection.html (noting 56 million cards were compromised).

[4] The Home Depot, Inc., Form 10-Q, (Nov. 25, 2014), *available at* http://www.sec.gov/Archives/edgar/data/354950/000035495014000047/hd_10qx11022014.htm.

[5] Data Breach QuickView, Risk Based Security (Feb. 2015), *available at* https://www.riskbasedsecurity.com/reports/2014-YEDataBreachQuickView.pdf.

[6] *Is Your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness*, PONEMON INSTITUTE (Sept. 2014), http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf.

[7] The most common forms of attack vary by industry. *See* 2014 Data Breach Investigations Report, VERIZON, http://www.verizonenterprise.com/DBIR/2014/. Internal security teams can increasingly target their defenses to the most common forms of attacks for their industry.

I. Data Breach Notification Requirements Are Governed By Varying State Laws

There is no generally applicable federal data breach notification law. Instead, data breach notification is largely governed by a patchwork of state laws with broadly similar requirements. As of this writing, only three states do not have a data breach notification law.[8] Although there are differences between state laws, most define (1) who must comply, (2) what information is covered, (3) what constitutes an incident requiring notice, (4) the timing and method of notification, and (5) circumstances where a company is exempt. These statutes have not been heavily litigated, but it may be difficult to comply with the varying requirements without developing an understanding of applicable state laws and putting a plan in place for when a breach inevitably occurs.

Many states have modeled their data breach requirements after California's data breach law, so it serves as a useful example of some common provisions amongst various state laws. Under California law, "[a] person or business that conducts business" in the state and "owns or licenses computerized data that includes personal information" may be required to notify certain data subjects of a data breach.[9] The information covered by the statute is "personal information" of state residents.[10] One area of variation between states is what information is considered personal information. In California, this includes a social security number, state driver's license number or identification card number, account or card number with codes that permit access to a financial account, medical information, and health insurance information.[11] An incident triggers the notification requirement when "personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[12] When a notification is required, companies must make the disclosure "in the most expedient time possible and without unreasonable delay."[13] The notice must be written in plain language and inform the data subject of certain details about the incident.[14] States also vary on the form of notice required, but most allow written notice, electronic notice, or substitute notice when the cost of providing notice or number of persons affected are high.[15]

There are some common exceptions to these general requirements. First, many states, including California, only require notification for incidents that expose unencrypted data.[16]

---

[8] National Conference of State Legislatures, *Security Breach Notification Laws* (Jan. 12, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (listing Alabama, New Mexico, and South Dakota).

[9] Cal. Civ. Code § 1798.82(a).

[10] *Id.* § 1798.82(h)(1).

[11] *Id.* § 1798.82(h)(1).

[12] *Id.* § 1798.82(a). California, like many other states, also requires Attorney General notification under certain circumstances. *Id.* § 1798.82(f).

[13] *Id.* § 1798.82(a).

[14] *Id.* § 1798.82(d).

[15] *Id.* § 1798.82(j).

[16] *Id.* § 1798.82(a).

Second, many states allow companies to delay notification at the request of law enforcement to aid a criminal investigation and so that a company can take measures to determine the scope of the breach and to restore system integrity.[17] Finally, the majority of states deem a company to have complied with notification requirements if it follows its own data breach notification policy and is otherwise consistent with timing requirements.[18]

In states that do not prescribe a specific number of days for notice, whether the timing of the notice is reasonable is a question of fact. In *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, the Southern District of California held that it could not resolve whether a ten-day delay in notifying PlayStation Network users was unreasonable as a matter of law at the motion to dismiss phase because that was a question for the trier of fact.[19] In its first motion to dismiss, Sony directed the court to the California Office of Privacy Protection's guidance on best practices following a data breach which stated that businesses should notify affected individuals within ten business days.[20] Although the court took judicial notice of the existence of the guidelines, it refused Sony's attempt to use them for a factual finding of reasonableness.[21]

The nature of existing statutes and case law suggest several practical steps that a corporate legal department can take to manage data breach notification requirements. Companies should evaluate how and when they can encrypt notice-triggering personal information to reduce the probability that a notice is required. Developing a written incident response plan as a part of their information security plan allows a company to take advantage of state laws that deem internal notification policies to comply with the requirement. Finally, determining, if practicable, the data breach statutes that are likely to apply can serve to limit the legal uncertainty inherent in this area of law.[22]

II. Reasonableness Is Driven By Context

Data breach litigation employs a reasonableness standard in many contexts but this standard is malleable and context-dependent.[23] A reasonableness standard appears in state[24] and

---

[17] *Id.* § 1798.82(a).

[18] *Id.* § 1798.82(k).

[19] *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 1009 (S.D. Cal. 2014).

[20] *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 973 (S.D. Cal. 2012).

[21] *Id.*

[22] For recommended best practices see California Office of Privacy Protection, *Recommended Practices on Notice of Security Breach Involving Personal Information* (Jan. 2012), *available at* http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/recom_breach_prac.pdf.

[23] *See* Peter Sloan, *The Reasonable Information Security Program*, 21 Rich. J.L. & Tech. 2, 3 (2014) ("Perhaps in recognition that security perfection is unattainable, information security laws share a common theme of reasonableness.").

[24] Under California's data security law, a business must "implement and maintain reasonable security procedures and practices appropriate to the nature of the information." Cal. Civ. Code § 1798.81.5(b). Other states have similar standards. *See, e.g.*, Ark. Code Ann. § 4-110-104(b).

federal[25] laws. Although questions of reasonableness appear in lawsuits between private parties,[26] this standard is most fully developed in FTC enforcement actions. But even in FTC actions this standard remains murky.

The FTC mandates "reasonable and appropriate" security measures to protect the security of its consumer data. Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[27] The Commission may only bring a claim under Section 5 when the practice is (1) likely to cause "substantial injury" to consumers, (2) the injury is not "reasonably avoidable" by consumers, and (3) bringing the claim is not "outweighed by countervailing benefits" to consumers.[28] The Commission has brought enforcement actions against companies for data breach vulnerabilities under both unfairness[29] and deception[30] theories when company practices were not deemed "reasonable and appropriate."

But what is "reasonable and appropriate" remains loosely defined because this determination is contingent on the context of a company's data collection and security practices. As the FTC recently explained:

> [t]he touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and

[25] Federal information security laws also evaluate data protection measures in terms of reasonableness. Under HIPAA, covered entities must "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity" of protected information and "[p]rotect against any reasonably anticipated uses or disclosures of such information that are not permitted or required." 45 C.F.R. § 164.306(a)(2)-(3). As a part of its flexible approach to data security HIPAA allows covered businesses to use any security measures that "reasonably and appropriately" implement the HIPAA security requirements. *Id.* § 164.306(b)(1).

[26] In *Patco Const. Co., Inc. v. People's United Bank*, the First Circuit found a bank's security system not commercially reasonable under Maine's implementation of the U.C.C. because it failed to incorporate one of many available security measures which could have prevented the fraud in the case. 684 F.3d 197, 210-11 (1st Cir. 2012). The court found that the bank could have used out-of-band authentication, user-selected pictures, physical tokens for generating one-time passwords, or monitoring and confirming high-risk transactions. *Id.* at 203-04. In contrast, the Eighth Circuit found a bank's security measures reasonable when it required users to create a user id and password, install authentication software that recorded information about the user's computer, allowed customers to place dollar limits on transactions, and allowed customers to require a second authorized user to approve a transaction. *Choice Escrow & Land Title, LLC v. BancorpSouth Bank*, 754 F.3d 611, 613-14 (8th Cir. 2014).

[27] 15 U.S.C. § 45(a)(1).

[28] *Id.* § 45(n).

[29] *See, e.g., FTC. v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR, at ¶¶ 24(a)-(j), 40 (D. Ariz. June 26, 2012) (alleging defendants "failed to provide reasonable and appropriate security for the personal information collected and maintained by [defendants]" and that "failure" "has caused and is likely to cause substantial consumer injury, including financial injury, to consumers and businesses," such as "compromise of more than 619,000 consumer payment card account numbers, the exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers' accounts, and more than $10.6 million in fraud loss").

[30] *See, e.g., In the Matter of GMR Transcription Services, Inc.*, No. C-4482, at ¶ 11 (FTC Compl., Aug. 14, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140821gmrcmpt.pdf (explaining that contrary to its representations GMR "engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security to protect personal information").

complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.[31]

The FTC's enforcement actions and consent orders do not themselves define reasonable practices, but they can help to explain the boundaries.[32] In recent Senate Committee testimony, the chairwoman of the FTC pointed to the enforcement action against TJX as a good example of the FTC's view on reasonableness in the data breach incidents.[33] In the FTC complaint against TJX, the commission alleged that the budget retailer failed to prevent a hacker from installing software that allowed the hacker to intercept and download payment card information resulting in millions of dollars in fraudulent charges and the exposure of personal information for 455,000 consumers.[34] The FTC claimed that TJX failed to employ "reasonable and appropriate" security measures for the personal information that it stored.[35] In the FTC settlement, TJX agreed to establish and maintain "a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information" it collects.[36] But the details of the security program were largely left undefined. TJX was required to designate employees responsible for the program, conduct a risk assessment with the consideration of some minimum risks, and adjust its program over time.[37] The FTC left it to TJX to design and implement "reasonable safeguards" to control the risks identified in its risk assessment and to develop "reasonable steps" to select and retain appropriate service providers.[38]

Because individual FTC consent orders and public statements cannot provide a comprehensive data security plan, companies are best served by following FTC guidance and weaving together FTC pronouncements in consent orders to get a broader sense of

---

[31] FTC, *Commission Statement Marking the FTC's 50th Data Security Settlement* (Jan. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

[32] Patricia Bailin, Study: *What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices*, THE PRIVACY ADVISOR (Sept. 19, 2014), https://privacyassociation.org/news/a/study-what-ftc-enforcement-actions-teach-us-about-the-features-of-reasonable-privacy-and-data-security-practices/ (discerning acceptable data security standards based on consent decrees).

[33] Edith Ramirez, Chairwoman, FTC, *Data Breach on the Rise: Protecting Personal Information From Harm* (Apr. 2, 2014), *available at* https://www.ftc.gov/system/files/documents/public_statements/296011/140402datasecurity.pdf.

[34] *In the Matter of The TJX Companies, Inc.*, No. C-4227, at ¶¶ 9, 11 (FTC Compl., July 29, 2008), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxcomplaint.pdf.

[35] *Id.* ¶ 8. In particular, the FTC faulted TJX for storing and transmitting personal information in clear text, failing to secure its wireless network with readily available security measures, failing to require employees to use strong passwords or different passwords across different systems, failing to use readily available security measures to protect its computers, and failed to use sufficient measures to detect, prevent, and investigate unauthorized access. *Id.*

[36] *In the Matter of The TJX Companies, Inc.*, No. C-4227, at 2 (July 29, 2008, Decision and Order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxdo.pdf.

[37] *Id.* at 3.

[38] *Id.*

reasonableness. The FTC, for example, issues guidance to help businesses develop and implement a data security plan.[39]

Recently, the FTC's authority to regulate data security practices under Section 5 powers has been called into question. In 2012, the FTC brought a Section 5 enforcement action against the hotel chain Wyndham, alleging it "failed to provide reasonable and appropriate security for the personal information" it collected.[40] Wyndham chose not to settle with the FTC and instead argued that the FTC's Section 5 authority does not cover data security because the overall statutory landscape shows Congress's intent to exclude data security from the agency's general jurisdiction over unfair and deceptive acts or practices.[41] The trial court judge denied Wyndham's motion to dismiss, but an interlocutory appeal of the order denying the motion to dismiss is currently under consideration by the Third Circuit.[42] This pending appeal, as well as proposed legislation explicitly granting the FTC authority to regulate data security, leave the future of FTC enforcement actions uncertain.

Whether or not the FTC retains enforcement jurisdiction over data breach, the issue of reasonableness will remain a large factor in determining a company's liability after a security incident because the concept is so ubiquitous in data breach law. Therefore, in-house counsel and data security teams should regularly evaluate the type of data stored, threats to that data, and precautions that are appropriate to the business.

III. Many Breaches May Lack Cognizable Injuries To Support Civil Actions

Even when a company does not reasonably secure data, it may be difficult for civil plaintiffs to establish a judicially cognizable injury. Because the FTC is unlikely to bring an enforcement action when the consumer injury is unclear,[43] this issue is more pertinent to the civil litigation context. Plaintiffs may find their claims barred by Article III standing requirements or they may find their substantive claims dismissed for lack of injury.

---

[39] The commission has explained five guiding principles to protecting consumer information in its publication, *Protecting Personal Information: A Guide for Business*. A company should (1) know what consumer information it possesses, (2) limit information collected and retained based on legitimate business needs, (3) protect information maintained by the company, (4) dispose of information when no longer needed, and (5) have a plan in place for a data breach incident. FTC, *Protecting Personal Information: A Guide for Business* (Nov. 2011), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

[40] *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 608 (D.N.J. 2014).

[41] *Id*. at 610-13.

[42] *See* Brief for FTC , *FTC v. Wyndham Worldwide Corp.*, No. 14-3514 (3d Cir. Nov. 5, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141105wyndham_3cir_ftcbrief.pdf.

[43] Closing letter, *Monster Worldwide, Inc.*, at 2 (Mar. 6, 2008), *available at* https://www.ftc.gov/sites/default/files/documents/closing_letters/monster-worldwide-inc./monsterworldwide.pdf (stating factors considered included, *inter alia*, the level of consumer injury and the type of information disclosed).

Standing presents a potential barrier to access to courts for data breach plaintiffs when their personal information has been accessed but they have not been directly harmed.[44] In these cases, standing requires that a threatened future injury be "certainly impending." In the recent Supreme Court decision, *Clapper v. Amnesty International*, the Court held that a plaintiff lacks Article III standing where future injury was too speculative to be considered certainly impending.[45] Although *Clapper* involved government surveillance and not data breach, a number of lower courts have applied this holding to dismiss data breach cases where a plaintiff's only injury is the increased risk of fraud or identity theft or from the costs associated with mitigating that risk.[46] But not all courts have found that *Clapper* forecloses standing.[47] In *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, the Southern District of California held that *Clapper* was consistent with existing Ninth Circuit precedent, and a plaintiff could establish standing where their personal data was exposed, as opposed to merely collected.[48] Likewise, in *In re Adobe Sys., Inc. Privacy Litig.*, Judge Koh found that *Clapper* did not change existing Ninth Circuit law on Article III's requirements.[49] Even if *Clapper* changed the requirements of standing, the court found the facts distinguishable because in a data breach "there is no need to speculate as to whether Plaintiffs' information has been stolen and what information was taken."[50] While it is too early to say whether courts will continue to apply *Clapper* to regularly deny Article III standing to data breach plaintiffs, this is a space to watch.[51]

---

[44] Plaintiffs have been unsuccessful in persuading courts that untimely notice under a data breach notification statute itself is a sufficient injury in fact to confer Article III standing. *See, e.g.*, *In re Adobe Sys., Inc. Privacy Litig.*, No. 13-CV-05226-LHK, 2014 WL 4379916, at *5 (N.D. Cal. Sept. 4, 2014) ("Plaintiffs do not have standing to bring a claim based on Adobe's alleged violation of Section 1798.82 (the notification provision), because Plaintiffs do not allege that they suffered any particular injury stemming from Adobe's failure to reasonably *notify* Plaintiffs of the 2013 data breach.").

[45] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143 (2013).

[46] *See, e.g.*, *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 28 (D.D.C. 2014); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 657 (S.D. Ohio 2014); *In re Barnes & Noble Pin Pad Litig.*, No. 12-CV-8617, 2013 WL 4759588, at *4-5 (N.D. Ill. Sept. 3, 2013).

[47] *See, e.g.*, *Moyer v. Michaels Stores, Inc.*, No. 14 C 561, 2014 WL 3511500, at *5-6 (N.D. Ill. July 14, 2014). In particular, the *Moyer* court noted that a subsequent Supreme Court ruling outside of the national security context appeared to apply a "less demanding" imminence requirement. *Id.* at *5.

[48] *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 961-62 (S.D. Cal. 2014).

[49] *In re Adobe Sys., Inc. Privacy Litig.*, No. 13-CV-05226-LHK, 2014 WL 4379916, at *7 (N.D. Cal. Sept. 4, 2014).

[50] *Id.* at *8.

[51] The Supreme Court has docketed a petition for certiorari in *Robins v. Spokeo*, on a related Article III standing issue. *Robins v. Spokeo, Inc.*, 742 F.3d 409 (9th Cir. 2014), *appeal docketed*, No. 13-1339 (2014). The question presented on appeal is whether Congress may confer Article III standing by authorizing a private right of action in the absence of concrete harm. Petition for a Writ of Certiorari, *Spokeo, Inc. v. Robins*, No. 13-1339 (U.S. May 2014), *available at* http://sblog.s3.amazonaws.com/wp-content/uploads/2014/05/13-1339-Spokeo-v-Robins-Cert-Petition-for-filing.pdf. Some technology companies have argued that the Ninth Circuit ruling, if allowed to stand, could open Article III jurisdiction without injury under federal and state laws. Brief for Amici Curiae eBay Inc., Facebook, Inc., Google Inc., and Yahoo! Inc. in Support of Petitioner, *Spokeo, Inc. v. Robins*, No. 13-1339 (U.S. June 2014), *available at* http://sblog.s3.amazonaws.com/wp-content/uploads/2014/06/13-1339-Spokeo-Inc.-v.-Robins-Br.-for-Amici-eBay-Inc.-et-al.-Jun....pdf.

And even where plaintiffs have alleged sufficient injury to satisfy Article III, they may still face difficulties pleading cognizable harm to state a claim. Plaintiffs typically invoke a host of statutory and common law claims in connection with data breaches but they often have difficulty establishing a cognizable injury that was caused by the breach. For instance, a number of cases interpreting data breach notification laws have found that there was no harm *resulting from the delay* to have a viable cause of action. Interpreting the Louisiana data breach law, the Middle District of Louisiana found that even an alleged nine week delay was not actionable without some damages resulting from the delay.[52] But that does not mean that a delay cannot be associated with an injury. In the recent Target litigation, the District of Minnesota denied Target's motion to dismiss with respect to 26 data breach notification violation claims, where the alleged damage was that consumers would not have shopped at Target had they known of the breach.[53]

Although plaintiffs assert many different theories of liability, they will often fail at the motion to dismiss phase without concrete injuries. For example, as the *In Re Sony* court recognized, present, non-speculative, harm is an essential element of a negligence claim under California law.[54] Many states also bar common-law negligence claims under the economic loss doctrine.[55] The doctrine bars a plaintiff from recovering for purely economic losses under a negligence theory under the theory that these losses should be recoverable, if at all, under a contract theory or the UCC.[56] Therefore, in states that recognize this doctrine, recovery for steps taken to avoid harm, such as credit monitoring services, may be barred under a negligence theory.[57]

The issue of cognizable injuries and non-speculative damages resonates with courts because they do not want to open the courthouse doors to intangible harms. Knowing this, in-house counsel should seek first to protect data that can cause immediate harm and seek to

---

[52] *Ponder v. Pfizer, Inc.*, 522 F. Supp. 2d 793, 796-98 (M.D. La. 2007); *see also In re Adobe Sys., Inc. Privacy Litig.*, No. 13-CV-05226-LHK, 2014 WL 4379916, at *10 (N.D. Cal. Sept. 4, 2014) (noting that cognizable harm from the failure to reasonably notify a data subject of a data breach is only the "incremental harm as a result of the delay"); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 31 (D.D.C. 2014) (requiring "independent harm caused by the delay"); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 1010 (S.D. Cal. 2014) ("plaintiff must allege actual damages flowing from the unreasonable delay"); *In re Barnes & Noble Pin Pad Litig.*, No. 12-CV-8617, 2013 WL 4759588, at *3 (N.D. Ill. Sept. 3, 2013).

[53] *In re Target Corp. Customer Data Sec. Breach Litig.*, No. MDL 14-2522 PAM/JJK, 2014 WL 7192478, at *9-10 (D. Minn. Dec. 18, 2014).

[54] "The breach of a duty causing only speculative harm or the threat of future harm does not normally suffice to create a cause of action for negligence." *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 962-63 (S.D. Cal. 2012).

[55] *See In re Target Corp. Customer Data Sec. Breach Litig.*, No. MDL 14-2522 PAM/JJK, 2014 WL 7192478, at *15-20 (D. Minn. Dec. 18, 2014) (analyzing the effect of economic loss doctrine for ten states and the District of Columbia).

[56] *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 528 (N.D. Ill. 2011).

[57] *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 960 (S.D. Cal. 2012).

mitigate security incidents before unauthorized access to innocuous data becomes harmful to customers.

IV. Different Types Of Data Receive Different Protection

In-house counsel should take note of the type of data their company is collecting because different types of data must be treated differently. There are state and federal laws which govern the manner in which different types of data must be handled. The type of data a company keeps will also affect the reasonableness of their data security practices and the type of injury that could result from unauthorized access.

Some laws provide specific data security regimes based on the data owner, data subject, or data type. The Gramm-Leach-Bliley Act provides security requirements for non-bank financial institutions.[58] The Fair Credit Reporting Act applies to credit reporting agencies.[59] The Children's Online Privacy Protection Act applies to data from children collected online.[60] Personal health information data security requirements in the Health Insurance Portability and Accountability Act apply only to covered entities such as health plans and providers.[61] Some state laws also require additional security measures for specific types of data.[62]

The type of data also will affect what precautions are reasonable. A credit card number or social security number generally should be handled with more secure systems than basic consumer information, such as names. This common sense notion can translate into a higher standard of reasonableness. For payment card information, a court may look to industry standards. For example, in *Michaels*, a retailer used non-payment card industry (PCI) compliant pin pads to process credit and debit card transactions, allowing unauthorized access to payment information by card skimmers.[63] The court applied PCI standards to find that the defendant had an obligation to implement procedures and practices that prevent skimmers from replacing legitimate devices with counterfeit machines.[64] In another example, the FTC closed an investigation against Monster Worldwide, Inc. without filing any charges against the company in part because it did not involve "inherently sensitive personal information such as Social Security numbers and credit card numbers."[65] Unauthorized hackers obtained names, phone numbers, and email addresses of Monster users, which they used for a targeted phishing campaign.[66]

---

[58] 15 U.S.C. § 6801 *et seq.*

[59] 15 U.S.C. § 1681 *et seq.*

[60] 15 U.S.C. § 6501 *et seq.*

[61] *See* 45 C.F.R. § 160.102.

[62] *See, e.g.*, Nev. Rev. Stat. § 603A.215(1) (requiring companies that collect payment cards to comply with PCI standards).

[63] *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 521-22 (N.D. Ill. 2011).

[64] *Id.* at 526.

[65] Closing letter, *Monster Worldwide, Inc.*, at 2 (Mar. 6, 2008), *available at* https://www.ftc.gov/sites/default/files/documents/closing_letters/monster-worldwide-inc./monsterworldwide.pdf

[66] *Id.* at 1.

Although these could be used to further other schemes, it was not as directly harmful as payment card information or social security numbers.

Similarly, a court is less likely to find causation when a data breach exposes less sensitive personal information that cannot be used to engage in fraud. In *SAIC*, the court dismissed a number of claims because of the nature of the data stolen.[67] A thief stole data tapes from a government service provider containing names, social security numbers, addresses, dates of birth, phone numbers, and medical information.[68] But the court dismissed several claims because of the nature of the data stolen and the alleged harm. The court dismissed identity theft claims because the data tapes did not contain credit card, debit card, or bank account information.[69] The court also dismissed privacy claims stemming from unsolicited marketing calls except where causation was not in doubt because the calls were to an unlisted number and targeted the plaintiff's specific medical condition.[70]

Knowing what data a company currently keeps is a part of a sound data security plan. Corporate counsel should understand the data a company keeps, ensure that heightened protection is in place where appropriate, and plan for how it must respond if and when there is a security incident.

V. Insurance Is Still A Gamble

Corporate counsel should analyze their current insurance coverage and assess the risks of data breach given their data use before purchasing additional insurance specifically for a data breach. One of the emerging trends in data breach law is the use of data breach insurance.[71] Because insurers still do not have abundant data to model the costs of data breach coverage, insurance products are still evolving and have different coverage and exclusions. But there is still uncertainty surrounding the scope of coverage in a data breach incident from a standard business insurance policy.[72] As the scope of coverage of general insurance policies is resolved, companies should carefully evaluate data breach insurance policies to determine whether this coverage is advisable, based on anticipated security threats to the company.

---

[67] *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 19-20 (D.D.C. 2014).

[68] *Id.* at *20.

[69] *Id.* at *31.

[70] *Id. at* *33.

[71] For example, Target maintains $100 million in "network-security" insurance coverage and expects to recover $90 million from its data breach incident, leaving the corporation with a net expense of $162 million. Target Corp., Form 10-K, (Mar. 13, 2015), *available at* http://investors.target.com/phoenix.zhtml?c=65828&p=irol-SECText&TEXT=aHR0cDovL2FwaS50ZW5rd2l6YXJkLmNvbS9maWxpbmcueG1sP2lwYWdlPTEwMTQ2Njc4JkRTRVE9MCZTRVE9MCZTUURFU0M9U0VDVElPTl9FTlRJUkUmc3Vic2lkPTU3.

[72] It appears likely that data breach exclusion endorsements will narrow the scope of data breach coverage under commercial general liability insurance policies. Roberta Anderson, *Coming To A CGL Policy Near You: Data Breach Exclusions*, Law360 (Apr. 23, 2014), http://www.law360.com/articles/529464/coming-to-a-cgl-policy-near-you-data-breach-exclusions.

Companies can purchase a variety of data breach insurance products that cover different costs associated with a data breach. Breach response policies cover costs associated with responding to, investigating, and remedying a data breach incident.[73] Third-party insurance covers losses arising from claims against a company from data subjects and the government.[74] Under either of these cyber insurance policies, companies should be careful to scrutinize the scope of coverage, exclusions, and duties of the insured because there is still significant variation between policies in this area.

The scope of insurance coverage for a data breach remains an open issue. Some losses arising from a data breach are arguably within the scope of standard insurance.[75] Sony has argued, thus far unsuccessfully, that costs arising from its PlayStation Network breach should be covered by general commercial liability policies.[76] But a case before the Connecticut Supreme Court raises questions about when insurance coverage will cover losses associated with a data breach. In *Recall*, tapes containing the data for 500,000 IBM employees fell off the back of a van on a highway exit ramp and were never recovered.[77] At issue is whether a clause in a company's general commercial liability insurance requiring "publication" for coverage was satisfied even though there was no evidence that IBM employees had suffered injury as a result of the loss of data.[78] The Connecticut intermediate appellate court agreed with the trial court and found that there was no publication, and the Connecticut Supreme Court has since agreed to review the decision.[79] A narrow definition of "publication" could mean that an insured will be denied coverage under general commercial liability insurance in these circumstances. More worryingly, insurers might also deny coverage under data breach insurance policies that require "access" if data is taken without evidence of use.[80] However, even if the Connecticut Supreme Court affirms the decision, the facts of this case will likely be distinguishable from typical data breaches where there is significant evidence of access.[81]

Given the evolving nature of insurance coverage in this area, corporate counsel should carefully evaluate the language in their existing and potential insurance policies. Careful consideration of the included coverage and exceptions should reduce the risk of not having coverage when you need it most.

---

[73] J. Andrew Moss, Cristina M. Shea, & David E. Weiss, *Fall Back On Insurance For Data Breach Fallout*, Law360 (Sept. 5, 2014), http://www.law360.com/articles/573832/fall-back-on-insurance-for-data-breach-fallout.

[74] *Id.*

[75] *Id.*

[76] Jeff Sistrunk, *Sony Coverage Denial Was Right Call, Insurance Groups Say*, Law360 (Jan. 29, 2015), http://www.law360.com/articles/616499/sony-coverage-denial-was-right-call-insurance-groups-say.

[77] *Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 147 Conn. App. 450, 453, 83 A.3d 664, 667 (2014).

[78] *Id.* at 463-64, 673.

[79] *Id.*

[80] Jeff Sistrunk, *Conn. High Court Case May Reshape Data Breach Coverage*, Law360 (Feb. 19, 2015) http://www.law360.com/articles/623080/conn-high-court-case-may-reshape-data-breach-coverage.

[81] *Id.*

VI. Takeaways

The risk of data breach increases every year and for corporate counsel, it is not a question of if, but when there will be a data security incident. The FTC has acknowledged that even a reasonable and appropriate data security program can be the victim of such an attack, so a data breach by itself does not mean there has been a breach of legal obligations. While reasonable safeguards may not prevent a company from having to defend itself in litigation, prudent steps taken before a breach can mitigate the potential exposure for a company that is the victim of such an attack.[82]

Advanced planning is critical:

- Companies should evaluate the data that they hold. Where are data subjects located? Is the data sensitive? Is the data subject to different treatment?
- Companies should evaluate whether they fall into a different regulatory regime. Are there industry-specific regulations? Does company-held data require different treatment?
- Companies should evaluate what precautions they currently take and whether they are reasonable. Do the security measures meet state or industry guidance? Do the measures meet prior representations?
- Companies should evaluate the risks. Will customers be harmed by the release of data? Is data breach insurance a sensible expenditure given its limitations?

There is no one-size-fits-all answer to these questions but there is no better time than now, before the inevitable incident, to plan.

[82] There are a number of other potentially important considerations beyond the guidance contained or referenced in this paper. For example, companies can consider entering into contracts with binding arbitration provisions and class action waivers to reduce the risk of a collective action and companies can build data security protocols and breach liability into service provider contracts. This discussion is intended as a broad overview, not a step-by-step roadmap for a complete data security plan.