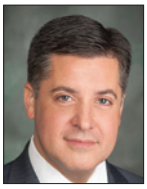
New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 257—NO. 81
FRIDAY, APRIL 28, 2017

Outside Counsel

Expert Analysis

So You've Been Hacked: The Changing Landscape of Post-Data Breach Liability



By **Joseph Facciponti**

And **Joseph Moreno**

The impact of serious data breaches are becoming both more common and more costly for businesses with each major attack. According to the New York State Attorney General, businesses reported 1,300 data breaches in 2016—a 60 percent increase from the prior year—that involved the personal data of 1.6 million New Yorkers.[1] Further, a 2016 independent data breach study conducted by the Ponemon Institute estimated that the average cost of a data breach to a U.S. corporation is roughly $7 million, a 29 percent increase since 2013.[2] When companies find themselves to be victims of a data breach, they must navigate an ever-expanding minefield of complex reputational, regulatory, and legal challenges. This article focuses on the potential for regulatory and civil liability for corporations in the aftermath of a data breach.

Regulatory Exposure

The recent trend has been for federal regulators, such as the Federal Trade Commission (FTC) and, more recently, the Securities and Exchange Commission (SEC), to treat hacked corporations less like victims and more like potential wrongdoers. This view is especially prevalent where the regulator concludes that the hacked corporation ignored red flags or failed to take appropriate precautions to protect sensitive data from theft. Despite the Trump Administration's general pro-business posture, federal and state regulators are displaying an increasing interest in being seen as aggressive in this space.

Federal Trade Commission. For several years, the FTC has actively sought to hold corporations across industry groups accountable for failing to protect their customers' private data. Section 5(a) of the Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[3] The FTC has applied this statute in enforcement actions against corporations for failing to adopt appropriate data protection programs or making misleading statements about the measures taken to protect customers' personal data—even in circumstances in which a corporation has not actually suffered a data breach. For example, in early January 2017, the FTC brought an enforcement action against D-Link, a manufacturer of Internet-enabled security cameras and devices, for allegedly failing to take steps to address security flaws in its equipment that could, for example, allow a hacker to access images from home security cameras, and also for misleading consumers about the security features of its products.[4] Since 2001, the FTC has pursued enforcement actions against nearly 60 corporations for failing to provide reasonable protections for consumers' personal information.[5]

When companies find themselves to be victims of a data breach, they must navigate an ever-expanding minefield of complex reputational, regulatory, and legal challenges.

Resolutions of FTC enforcement actions typically involve a combination of fines and mandates for companies to improve their data security practices. In 2010, the FTC entered into a settlement with LifeLock—a company that specializes in providing data protection services to

JOSEPH FACCIPONTI *is a special counsel in Cadwalader, Wickersham & Taft's New York office and a former Assistant U.S. Attorney for the Southern District of New York.* JOSEPH MORENO *is a partner in the firm's white-collar defense and investigations group and served at the U.S. Department of Justice in the National Security Division's Counterterrorism Section.*

consumers—for deceptive advertising and failing to secure its own customers' personal information, including their social security, credit card, and bank account numbers. When LifeLock subsequently violated the terms of the settlement by failing to establish a comprehensive information security program, the FTC pursued contempt proceedings and LifeLock ultimately was required to pay a $100 million penalty in 2015—one of the largest ever obtained by the FTC in an enforcement action.[6]

Recent developments raise questions regarding the FTC's ability and willingness to continue this aggressive approach. First, a challenge to the FTC's authority to bring cases under §5(a) of the FTC Act is currently pending before the Eleventh Circuit. Among the issues on appeal in that case is whether the FTC has authority to pursue enforcement under §5(a) of the FTC Act if consumers have not suffered a tangible injury as a result of a company's failure to secure their data. In a preliminary opinion granting a stay of the FTC's decision in the matter, the Eleventh Circuit held that LabMD, a now-defunct medical testing company that inadvertently caused records related to over 9,000 patients to be available over the internet, had raised "compelling reasons" why the FTC's interpretation of §5(a) might be unreasonable.[7]

Second, whether the FTC under the Trump Administration will continue to vigorously pursue enforcement actions remains to be seen. Earlier this year, President Trump named FTC Commissioner Maureen K. Ohlhausen as Acting Chairperson. In a speech to the American Bar Association's Consumer Protection Conference on Feb. 2, 2017, Ohlhausen stated the FTC should focus on cases with "objective, concrete harms such as monetary injury and unwarranted health and safety risks," not on those involving "speculative injury."[8] Ohlhausen also has a history of dissenting from some of the FTC's more aggressive actions, including the action filed against D-Link and the contempt finding against LifeLock, with which she took issue due to a lack of evidence that any of LifeLock's customers' data actually was stolen.[9]

Securities and Exchange Commission. It is also an open question whether the SEC will continue to aggressively pursue enforcement actions against corporate hacking victims, particularly in light of statements by President Trump's nominee for Chairman, Jay Clayton, that companies should not be shouldered with government-imposed cybersecurity mandates or take the blame for data breaches conducted by actual cybercriminals who are often unreachable by law enforcement.[10]

> For companies already dealing with a multitude of regulatory regimes including foreign bribery, money laundering, and economic sanctions, it is clear that developing a robust cybersecurity compliance program also must be a priority.

Under Regulation S-P, the so-called "Safeguards Rule," which was promulgated under §504 of the Gramm-Leach-Bliley Act, registered broker-dealers, investment companies, and investment advisers are required to adopt policies and procedures to prevent unauthorized access or use of customer data that could result in substantial harm or inconvenience to a customer.[11] In 2016, the SEC fined a major financial institution $1 million for a data breach in which a rogue employee stole data related to hundreds of thousands of customer accounts.[12] The stolen data ultimately found its way online—possibly because the employee himself was hacked. The bank took prompt action to investigate the incident and remove the data from the Internet, alert the SEC and its customers, remediate the security issue, and terminate the rogue employee who was ultimately prosecuted by the Department of Justice. Nonetheless, the SEC determined that the bank did not, among other things, properly test its system for security weaknesses or effectively monitor its system for unusual or suspicious activity, and, therefore, was subject to sanction under Regulation S-P.

Publicly-traded companies (issuers) also need to consider issues of disclosure with respect to data breaches, as failure to do so also can lead to SEC scrutiny. The SEC is reportedly investigating Yahoo! over the timing of its disclosures—which it did not make until 2016—of massive data breaches of user account names and passwords that occurred in 2013 and 2014 and that the company learned of in 2014.[13] Yahoo!'s delinquent disclosure also impacted its agreement to be purchased by Verizon, resulting in a reduction of the purchase price from $4.83 billion to $4.48 billion.[14]

Treasury Department. Under the Bank Secrecy Act, banks, broker-dealers, and other covered financial institutions have long been required to file Suspicious Activity Reports (SARs) with the Financial Crimes Enforcement Network (FinCEN) for transactions involving potentially suspicious activity. In 2016, FinCEN issued guidance requiring financial institutions to file SARs in cases of "cyber-events" that affect a transaction or series of transactions. The significance of FinCEN's action is that financial institutions now will have to incorporate cybersecurity incidents

into their existing financial crime and SAR compliance program.[15]

New York and Other State Regulators. Even if the federal government scales back its enforcement of data security regulations, state regulators are ready to step forward with their own stringent cybersecurity regulations. In New York, the Department of Financial Services (DFS) recently enacted its own cybersecurity rules for "covered entities," including banks, insurance companies and other regulated financial institutions.[16] The new rules went into effect on March 1, 2017, and require a host of cybersecurity risk management measures. These requirements include, among other things: appointing a Chief Information Security Officer; adopting comprehensive, board-approved cybersecurity policies and procedures; implementing technical measures such as using two-factor authentication and encrypting confidential data; providing procedures to manage third-party cybersecurity risk; requiring the reporting of cybersecurity events to DFS within 72 hours of discovery; and requiring an annual certification of compliance by a senior officer. Although it remains to be seen how stridently DFS will enforce the new rules, it is known for its aggressive posture in other areas such as money laundering.

While New York has touted its "first-in-nation" cyber rules, other states are bound to be close behind.

European Data Privacy Rules. In addition to the growing regime of federal and state regulations in the United States, the European Union's General Data Privacy Directive (GDPR) will go into effect in May 2018.[17] The GDPR applies to any business, including U.S. companies, that solicit customers in Europe, and requires, among other things, strict protection of customer confidential data; implementation of data protection policies and procedures; prompt reporting—within 72 hours—of a data breach to regulators and, without undue delay, to affected customers; and the appointment, in certain circumstances, of a Data Protection Officer. Failure to comply could result in the imposition of fines of up to the higher of four percent of worldwide annual turnover of the business, or €20 million (approximately $21 million).

Civil Liability

Businesses that have suffered data breaches also face potential civil liability from a host of potential plaintiffs, including customers, credit card issuers, business partners, and shareholders.

Consumer Class Action Suits. For consumers whose personal data—such as Social Security or driver's license numbers, credit card or bank account information, or passwords and security question answers—is compromised in a data breach, the primary challenge in civil litigation has historically been to establish an injury-in-fact sufficient to establish standing. Federal courts have struggled with whether a plaintiff had standing in cases where personal data was hacked, but where there was no affirmative misuse of that data that resulted in economic or other tangible harm to the consumer. The issue also arose in cases where a cyberthief used stolen credit card or bank account information to make fraudulent purchases or withdrawals, but where the consumer was fully reimbursed for those losses by their bank or credit card issuer and again suffered no pecuniary loss.

In May 2016, the U.S. Supreme Court addressed the issue of standing in *Spokeo, Inc. v. Robins*.[18] *Spokeo* did not involve a data breach per se, but an allegation that the defendant, which provides biographical information about individuals on the Internet, had violated the Fair Credit Reporting Act (FCRA) by publicly published inaccurate information about the plaintiff. The *Spokeo* court held against the plaintiff, finding that a bare statutory violation was insufficient to confer standing unless the plaintiff had also suffered injuries that were both "particularized" *and* "concrete." The court remanded the case, directing the Ninth Circuit to consider whether the plaintiff's alleged injury was "concrete."

Since the *Spokeo* decision, however, the Third and Sixth Circuits have found instances in which plaintiffs have standing in the context of a data breach. In *Galaria v. Nationwide Mut. Ins. Co.*, the Court of Appeals for the Sixth Circuit held that where plaintiffs incurred mitigation costs as a result of a data breach—including credit and identity-theft monitoring and credit freezes—they had satisfied the injury requirement of standing.[19] In *In re Horizon Healthcare Services Data Breach Litigation*, the Third Circuit held that unauthorized dissemination of plaintiffs' confidential information was itself a sufficiently concrete injury under the FCRA to confer standing.[20] Further, the Seventh Circuit, in an opinion issued just before the *Spokeo* decision, also held that the increased risk of fraudulent charges by identity thieves is sufficient to confer standing, since a primary incentive for hackers is to make fraudulent use of stolen data.[21] However, not all Courts of Appeals are aligned: In *Beck v. McDonald*, the Fourth Circuit came to the opposite conclusion, holding that increased risk of identity theft from a data breach is not sufficient to establish standing, particularly where the passage of years since the data breach revealed no evidence that the plaintiffs' identities have been affirmatively misused.[22]

In major data breach cases where consumer plaintiffs have survived a motion to dismiss, they have frequently been able to extract seven-figure settlements and other concessions. For example, in 2016, Home Depot agreed to pay up to $19.5 million to settle consumer class action claims arising from the 2014 theft of credit and debit card records for approximately 50 million customers in addition to over $7.5 million in legal fees and costs for plaintiffs.[23] In particular, the settlement provided for credit monitoring and up to $10,000 for cardholders with valid claims. In 2017, Neiman Marcus agreed to pay $1.6 million to settle a consumer class action lawsuit arising from the theft of credit card information for approximately 350,000 consumers, and also agreed to make changes to its data security practices including the use of chip-based payment card infrastructure and improved education and training of employees on privacy and data security matters.[24]

Banks and Credit Card Issuers. Credit and debit card issuers historically have had less difficulty establishing standing and obtaining even greater settlement amounts, as they often bear the ultimate financial loss from the theft of credit and debit card information due to their reimbursement to cardholder victims. Accordingly, for example, Target reportedly agreed to pay over $100 million in various settlements with Visa, MasterCard, and card issuers for a 2013 data breach that involved the theft of as many as 40 million credit cards.[25]

Shareholder Derivative Actions. Shareholder derivative lawsuits in response to data breaches have had the least success to date. In 2014, a derivative lawsuit filed against Wyndham Worldwide Corporation's board of directors over a series of data breaches between 2008 and 2010 was dismissed by a federal district court judge in New Jersey, who held that the board's actions taken in response to the breaches were a good-faith exercise of business judgment as required by Delaware law.[26] Shareholder derivative suits brought against Target[27] and Home Depot[28] for data breaches have been similarly dismissed. However, even if these types of derivative lawsuits against directors and officers continue to be unsuccessful, that may be small comfort to the corporate victims of hacking who are nonetheless required to expend time and resources responding to them.

Conclusion

For companies already dealing with a multitude of regulatory regimes including foreign bribery, money laundering, and economic sanctions, it is clear that developing a robust cybersecurity compliance program also must be a priority. This will have to include written policies and procedures, internal controls, employee training, independent auditing, and regular reporting to senior management and the board of directors. It also should incorporate a data breach response plan which incorporates not only IT steps, but also how to deal with the legal and public relations fallout of such an event. Failing to do so leaves companies open not only to serious reputational harm, but to regulatory scrutiny and potential civil litigation whose costs can easily become staggering.

1. See Press Release, "A.G. Schneiderman Announces Record Number of Data Breaches for 2016," N.Y. Office of the Attorney General (March 21, 2017).
2. See "2016 Cost of Data Breach Study: Global Analysis," Ponemon Institute LLC (June 2016).
3. Codified at 15 U.S.C. §45(a) & (n).
4. See Press Release, "FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras" (Jan. 5, 2017), Federal Trade Commission.
5. See Prepared Statement of the Federal Trade Commission before the House Committee on Small Business, "Small Business Cybersecurity: Federal Resources and Coordination" (March 8, 2017).
6. See Press Release, "LifeLock to Pay $100 Million to Consumers to Settle FTC Charges it Violated 2010 Order," Federal Trade Commission (Dec. 17, 2015).
7. See *LabMD v. Federal Trade Commission*, No. 16-16270, __ Fed. Appx. __, 2016 WL 8116800, at *3 (11th Cir. Nov. 10, 2016).
8. See Opening Keynote of Maureen K. Ohlhausen, ABA 2017 Consumer Protection Conference (Feb. 2, 2017).
9. See "Dissenting Statement of Commissioner Maureen K. Ohlhausen," *FTC v. LifeLock*, Matter No. X100023 (Dec. 17, 2015).
10. See Roger Yu, "Honed by Wall Street: What Makes Trump SEC Pick Jay Clayton Tick," USA Today (Jan. 4, 2017); Jay Clayton, David Lawrence & Frances Townsend, "We Don't Need a Crisis to Act Unitedly Against Cyber Threats," Knowledge@Wharton (June 2015).
11. Codified at 17 C.F.R. §248.30.
12. See SEC Press Release (June 8, 2016).
13. See Aruna Viswanatha and Robert McMillan, "Yahoo Faces SEC Probe Over Data Breaches," Wall Street Journal (Jan. 23, 2017).
14. See Irina Ivanova, "Verizon slashes offer price for Yahoo over data breaches," CBS News (Feb. 21, 2017).
15. See "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," Financial Crimes Enforcement Network (Oct. 25, 2016).
16. See 23 NYCRR 500.
17. See Directive 94/46/EC.
18. No. 13-1339, 136 S. Ct. 1540 (May 24, 2016).
19. See 663 Fed. Appx. 384 (6th Cir. 2016).
20. See *In re Horizon Healthcare Services Data Breach Litigation*, 846 F.3d 625 (3d Cir. 2017).
21. See *Lewert v. P.F. Chang's China Bistro*, 819 F.3d 963 (7th Cir. 2016).
22. See 848 F.3d 262 (4th Cir. 2017).
23. See Jonathan Stempel, "Home Depot settles big lawsuit over big 2014 data breach," Reuters (March 8, 2016); see also *In re Home Depot*, No 14-md-2583, ECF Nos. 260 & 261 (N.D. Ga. Aug. 23, 2016) (orders approving settlement agreement).
24. See Maria Halkias, "Neiman Marcus to pay $1.6 million in shopper data breach lawsuit," Dallas News (March 20, 2017); *Remijas v. The Neiman Marcus Group*, No. 14-cv-1735, ECF No. 145 (N.D. Ill. March 17, 2017) (Plaintiffs' Memorandum of Law in Support of Settlement and Class Certification).
25. Jonathan Stempel and Nandita Bose, "Target in $39.4 million settlement with banks over data breach," Reuters (Dec. 2, 2015).
26. See *Palkon v. Holmes, et al.*, No. 14-cv-1234, 2014 WL 5341880 (D.N.J. Oct. 20, 2014).
27. See Shayna Posses, "Target Execs Escape Derivative Claims Over Data Breach," Law360 (July 7, 2016).
28. See *In re The Home Depot Shareholder Derivative Litig.*, No. 15-cv-2999, 2016 WL 6995676 (N.D. Ga. Nov. 30, 2016).