Client Advisory

CARTER LEDYARD & MILBURN LLP
Partners for Your Business®

Litigation Department & Cybersecurity Practice Group

April 26, 2017

Cybersecurity: Regulatory and Litigation Consequences of a Data Breach

2016 was a record year for cybersecurity breaches and threats, as hackers and cyber-criminals continued to employ sophisticated strategies to access data. In 2016, 4,149 cybersecurity breaches were publicly reported, involving unauthorized access to or disclosure of over 4.2 billion records.[1] Breaches have involved personal information, such as social security numbers, passwords, and health-related information; financial information of consumers and customers, such as credit card numbers and bank account information; and confidential business information, such as trade secrets and other sensitive or valuable data. Victims of cybersecurity attacks have included global law firms, Fortune 500 companies, and government agencies. No one is immune from attack. Small entities that do not have a dedicated IT staff (such as nonprofits, which may possess sensitive donor information) are particularly vulnerable to attacks.

Breaches may be caused by human or system error, however the majority of cybersecurity breaches are caused by planned attacks (including hacking, phishing, ransomware, or malware). It is critical that all companies (including small businesses, self-employed consultants, and even nonprofits) have cybersecurity measures in place (technical and procedural) to protect against data breaches. As cyber threats have increased, we have seen an increase in laws and regulations and rapidly evolving legal standards designed to force companies to improve their protections against such threats and minimize damages to third parties. Companies must take steps to understand and comply with the applicable state and federal laws and regulations and identify and address their cyber risks to avoid the legal consequences and costs associated with a data breach.

The costs associated with data breaches can be significant. One study suggests that the average organizational cost of a cybersecurity data breach for a U.S. company in 2016 was $7 million.[2] Costs include forensic investigation and remediation, identification of data breach victims, legal defense and strategy, communications and public relations, notice and reports to regulators and victims, training, and protection services offered to victims. Data breaches often lead to investigations by state or federal agencies; regulatory fines and sanctions; shareholder suits; and private litigation and class actions by consumers, clients, patients, and employees. It is

[1] Risk Based Security, *Data Breach QuickView Report: 2016 Data Breach Trends – Year in Review*, available at https://pages.riskbasedsecurity.com/2016-ye-breach-quickview.

[2] Ponemon Institute, *2016 Cost of Data Breach Study: Global Analysis* (June 2016), available at https://securityintelligence.com/media/2016-cost-data-breach-study/.

thus imperative that companies have informed counsel to advise them on legal preparation and strategies to prevent breaches and to react appropriately to breaches when they occur.

State Regulation and Enforcement

Forty-eight states, as well as the District of Columbia, have statutes requiring private or governmental entities to report and notify individuals of security breaches involving personally identifiable information ("PII"). State breach laws typically have provisions regarding who must comply with the law, definitions of applicable personal information, what constitutes a breach, notice and reporting requirements, and exemptions.

New York has had regulations in place for several years which require businesses to report security breaches of computerized PII. Recently, however, New York became the first state to implement more detailed regulations applicable to banks, insurers, and other covered entities. The New York Department of Financial Services ("DFS") regulations, titled *Cybersecurity Requirements for Financial Services Companies*, went into effect on March 1, 2017, and, among other things, require covered entities to appoint a Chief Information Security Officer ("CISO"), establish a written cybersecurity policy, conduct periodic risk assessments, and report cybersecurity events and breaches to DFS within 72 hours. These regulations are described in more detail in our *January 2017 advisory*.

State Attorneys General ("AGs") typically conduct investigations and enforcement actions relating to violations of state cybersecurity laws and regulations, and often cooperate on multi-state investigations and enforcement actions. In addition to the significant costs associated with investigating, remedying, and reporting cybersecurity breaches, companies may also receive fines or monetary penalties. The following are some recent examples of state enforcement actions and settlements:

- On January 26, 2017, *Acer Service Corporation* settled with the New York AG over an alleged data breach involving more than 35,000 credit card numbers, including the credit card information and other personal information of 2,250 New Yorkers. As part of the settlement, Acer agreed to pay $115,000 in penalties and to improve its data security practices.
- On September 30, 2016, the *Trump Hotel Collection* agreed to pay a fine of $50,000 and bolster its data security practices as part of a settlement with the New York AG involving a hack of the Soho and Trump International in New York (as well as other properties) that affected more than 70,000 credit card numbers and other personal data.
- On November 7, 2016, *Adobe Systems Inc.* settled with 15 state AGs relating to allegations that the company lacked proper measures to protect its systems from a 2013 cyber attack that resulted in the theft of the personal information of millions of customers. Adobe agreed to pay $1 million to the AGs and implement new data security policies and practices.

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

- On December 15, 2015, the California AG announced an approximately $25 million settlement with *Comcast Cable Communications, LLC* stemming from allegations that Comcast disposed of electronic equipment in landfills without properly deleting customer information from the equipment.

Federal Regulation and Enforcement

There is no comprehensive federal data privacy law. However, several federal laws and regulations have been interpreted to require that companies maintain the security of PII and report when breaches occur.

Federal Trade Commission ("FTC"). The FTC is the primary federal agency regulating consumer privacy and data security. The FTC is authorized to bring enforcement actions and issue civil penalties against entities engaged in unfair or deceptive trade practices, and has recently used this authority to bring actions against organizations that have violated consumers' privacy rights or misled them by failing to maintain security for sensitive consumer information. The FTC enforces a range of statutes and regulations, including the *Graham-Leach-Bliley Act* (requiring financial institutions to explain their information-sharing practices to customers and to safeguard sensitive data), the *Fair Credit Reporting Act* ("FCRA") (requiring that companies possessing or maintaining credit reporting information safeguard such information, and creating certain private causes of action), the *Children's Online Privacy Protection Act* ("COPPA") (requiring that entities collecting personal information from children under 13 years of age safeguard such information), and the *Fair and Accurate Credit Transactions Act* ("FACTA") (amending the FCRA to further prevent and mitigate identity theft and improve the accuracy of consumers' credit-related records). Entities that handle any type of consumer PII should consult the FTC's published guidance relating to cybersecurity measures, implementation of effective cybersecurity plans, and the reporting of breaches.[3]

Securities and Exchange Commission ("SEC") and Financial Industry Regulatory Authority ("FINRA"). *Regulation S-P* requires SEC-registered broker-dealers, investment companies, and SEC-registered investment advisers to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information." The SEC's Enforcement Division has brought enforcement actions against firms under *Regulation S-P* for the failure to safeguard client data. The SEC and FINRA have recently emphasized that their examinations of firms will focus on cybersecurity compliance and readiness. In addition, the SEC and FINRA have published guidance and best practices to be followed by banks, investment advisers, broker-dealers, and other securities industry firms to protect customer and client PII, respond to cybersecurity incidents, and report or disclose incidents when appropriate. And, although the SEC has not yet brought an enforcement action for failure to report a cyber incident, the SEC's acting Enforcement

[3] For example, see generally Federal Trade Commission, *Data Breach Response: A Guide for Business* (2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf, and Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

Director indicated this month that such an enforcement action "absolutely" could be envisioned. For more detailed information on guidance for broker dealers and investment advisers, see our *January 2017 advisory*.

Department of Health and Human Services ("HHS"). The 1996 *Health Insurance Portability and Accountability Act* ("HIPAA"), administered and enforced by the HHS, applies to health care providers, health care plans, and health care clearinghouses. It requires, among other things, that covered entities safeguard electronic protected health information ("ePHI"), conduct risk assessments, maintain policies and procedures, respond to and mitigate the effects of security breaches, and report breaches to the HHS and affected individuals. These regulations, and HIPAA guidance, are described in more detail in our *February 2017 advisory*. In the first four months of 2017, the HHS has already collected fines totaling over $14.3 million.[4]

Federal Communications Commission ("FCC"). The FCC regulates data privacy and security for telecommunications providers, including internet service providers, under the *Communications Act of 1934* and *Telephone Consumer Protection Act of 1991* ("TCPA"). In October 2016, it adopted regulations, entitled *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, intended to "give broadband consumers increased choice, transparency, and security over their personal data." These regulations require providers to (a) provide notice and choice to consumers of how data is collected and used, (b) take reasonable security measures to protect PII, and (c) report breaches to the FCC, affected consumers, and (in some cases) the FBI and Secret Service. The FCC may bring enforcement actions and issue fines and penalties. The TCPA also provides for a private cause of action.

The following are some recent examples of federal enforcement actions and settlements:

- In April 2015, *AT&T* agreed to pay $25 million to settle an FCC investigation into consumer privacy violations at AT&T's overseas call centers involving the unauthorized disclosure of almost 280,000 U.S. customers' names, full or partial Social Security numbers, and protected account-related data.
- In June 2016, *Morgan Stanley* agreed to pay a $1 million penalty to settle SEC claims related to its failure to protect customer PII. Over 730,000 customer accounts were improperly accessed and their data copied by a Morgan Stanley employee to his personal server, which was then hacked by a third-party who offered the PII for sale online.
- In August 2016, *Advocate Health Care* settled with the HHS for $5.55 million to resolve HIPAA violations relating to the disclosure of sensitive ePHI of approximately 4 million patients, which included a data breach of its subcontractor billing company that exposed such data.

[4] U.S. Dep't of Health and Human Services, *HIPAA News Releases & Bulletins* (April 25, 2017), available at https://www.hhs.gov/hipaa/newsroom/index.html.

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

- In December, 2016, operators of the *AshleyMadison.com* dating site settled with the FTC in connection with a large-scale hacking incident involving PII of 36 million users. The company agreed to pay $1.6 million and was required to implement a range of data security practices to better-protect its users' PII.

Private Litigation

In addition to the regulatory consequences, breaches may lead to a variety of private suits. Employees, customers, clients, and patients whose information is exposed may bring individual or class action suits under many causes of action, including breach of privacy, negligence, breach of contract, and violations of federal or state statutes. Financial institutions and credit card companies that have incurred expenses (for unauthorized charges or increased fraud monitoring) as a result of a data breach may seek damages from the entity that was the victim of the breach. In addition, shareholders may bring derivative suits against directors and officers alleging breach of fiduciary duty and corporate waste.

One of the major hurdles for consumer-plaintiffs is satisfying the burden to show concrete injury as a result of the breach. This past year, the U.S. Supreme Court, in *Spokeo Inc. v. Robins*, 136 S. Ct. 1540, 1549-50 (2016), decided that a plaintiff must suffer an injury in fact that is both particularized and concrete in order to have standing to sue under Article III of the U.S. Constitution, "even in the context of a statutory violation." However, the *Spokeo* decision offers little guidance as to which injuries are sufficiently concrete. The Court remanded the case to the Ninth Circuit to determine whether the dissemination of inaccurate information about Robins by Spokeo, a people search engine, constituted sufficiently concrete harm for Robins to have standing to sue Spokeo for alleged violations of the FCRA. The Ninth Circuit heard oral arguments in December 2016.

In the months since the *Spokeo* decision, lower courts have issued contradictory interpretations with respect to many legal claims in data breach litigation. For example, the Sixth and Seventh Circuits have issued decisions finding that the risk of future harm from identity theft and related fraud-prevention expenses are sufficiently concrete harms to confer standing, whereas district courts in other circuits have held that the threat of future harm from identity theft is too speculative to confer standing. The Third Circuit, in *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, No. 15-2309, 2017 WL 242554, at *11 (3d Cir. Jan. 20, 2017), held that an alleged statutory violation of the FCRA's requirement to protect certain data is a sufficiently concrete harm to confer standing, whereas district courts in other circuits have held that an alleged statutory violation of FACTA's requirement to protect certain data, on its own, is insufficient to confer standing.[5]

Shareholder-plaintiffs also face an obstacle: the requirement that shareholders either have made a demand that the board take action or demonstrate that such a demand would have been futile. For instance, in November 2016, a suit filed by shareholders of Home Depot was dismissed by a district court in Georgia because the shareholders had not demanded that the board investigate its cybersecurity measures prior to the breach and had

[5] *See, e.g.*, *Noble v. Nev. Checker CAB Corp.*, No. 2:15-CV-02322-RCJ-VCF, 2016 WL 4432685, at *4 (D. Nev. Aug. 19, 2016), *appeal docketed*, No. 16-16573 (9th Cir. Sept. 7, 2016).

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

not shown particularized facts beyond a reasonable doubt that the board would have been unable or unwilling to evaluate such a demand in a disinterested manner.[6]

Despite the obstacles facing plaintiffs in data breach suits, many cases survive motions to dismiss in whole or in part. Defendants have been particularly unsuccessful in motions to dismiss suits by financial institutions, which are typically able to demonstrate particularized and concrete harm in the form of expenses related to fraudulent charges to customer accounts, notification of customers, and increased monitoring for fraudulent activity. Many cases are ultimately settled.

The following are additional examples of litigation involving data breach:

- *Home Depot* was the subject of a consumer class action consolidated in federal court in Georgia on behalf of approximately 56 million customers whose payment or contact information was exposed in a 2014 data breach. In August 2016, Home Depot agreed to pay a total of $19.5 million plus court costs and attorneys' fees to settle the suit.
- A class action was filed against *Target* in federal court in Minnesota by financial institutions seeking damages for their expenses in connection with a 2013 breach that exposed payment and contact information of millions of customers. Target agreed in May 2016 to pay $39 million plus costs and attorneys' fees, and separately settled with Visa for $67 million. Target settled a consumer class action arising from the same breach for $10 million.
- In 2012, approximately 100 million usernames and passwords were stolen from *LinkedIn*. In 2015, LinkedIn settled a resulting class action litigation filed in federal court in California for $1.25 million.
- *Sony* was the subject of an employee class action filed in federal court in California after employee personal information was accessed in a 2014 cyber attack. In April 2016, Sony settled the case, agreeing to cash payments to all class members, payment for identity protection services, and costs and attorneys' fees—a total estimated to be around $15 million. In July 2016, a movie producer sued Sony in federal court in Florida for breach of contract in connection with the same 2014 cyber attack, alleging that Sony violated a distribution agreement by failing to prevent piracy of the producer's films. In April 2017, the Court ordered the case to arbitration pursuant to a clause in the agreement.
- A class action was filed in state court in California on behalf of 31,074 patients of the *St. Joseph Health System* in connection with a 2012 breach of protected health information. The February 2016 settlement requires payment for credit monitoring services for the class, payment of $10.5 million plus costs and attorneys' fees, and promised changes to security practice—total costs exceeding $18 million.

---

[6] *In re The Home Depot, Inc. S'holder Derivative Litig.*, No. 1:15-cv-02999-TWT, 2016 U.S. Dist. LEXIS 164841 at *11–14 (N.D. Ga. Nov. 30, 2016), *appeal docketed*, No. 16-17742 (11th Cir. Dec. 28, 2016).

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

- In January 2016, *Wendy's* announced a breach affecting payment information from customers at over 1,000 restaurants. In February 2016, a consumer class action was filed in federal court in Florida on behalf of customers whose information was stolen. In March 2017, the court held that the plaintiffs had sufficiently alleged injuries to confer standing, and allowed the negligence and implied contract claims to move forward, but granted the motion to dismiss other claims based on state consumer protection laws and data breach statutes while allowing plaintiffs to replead such claims. Another class action was filed in August 2016 in federal court in Pennsylvania by 26 financial institutions seeking damages for their expenses resulting from the same breach. In addition, in December 2016, a shareholder filed a derivative suit in federal court in Ohio against the officers and directors of Wendy's claiming, among other things, breach of fiduciary duty and corporate waste.

Conclusion

Given the increased threat of cyber attacks, the massive amount of information that companies maintain in electronic form, and the significant costs that flow from a data breach (litigation, regulatory, and otherwise), it is important that companies be proactive in order to minimize risks and costs. Companies are encouraged to consult counsel regarding cybersecurity initiatives and may find the annexed list of best practices useful.

For more information concerning the matters discussed in this publication, please contact the authors **Matthew D. Dunn** (212-238-8706, mdunn@clm.com), **Melissa J. Erwin** (212-238-8622, erwin@clm.com), or **Kortni Hadley** (212-238-8871, hadley@clm.com); another member of CL&M's Cybersecurity Practice Group; or your regular CL&M attorney.

Appendix

Cybersecurity Best Practices

- Appoint a CISO or the equivalent.
- Conduct an organizational risk assessment, which entails the following:
    - identify the types of information maintained by the organization that may be prone to cybersecurity attacks and data breaches (personal and financial information, health information, trade secrets, etc.),
    - review existing cybersecurity policies or protections, and
    - conduct a risk assessment of third party vendors or professionals that have access to the organization's data, and request information about their cybersecurity program.
- Assess the state and federal regulations and laws that are applicable to an organization, and the related technical or reporting requirements.
- Establish a cybersecurity program that includes written policies addressing any applicable legal or regulatory requirements and an incident response plan which details steps to take in the event of a breach and allocates responsibilities to organization personnel.
- Ensure that personnel understand the cybersecurity policies and incident response plan and their obligations thereunder.
- Conduct periodic assessments of the cybersecurity program, including penetration testing, as well as periodic assessments of third party vendors or professionals.
- Consider the use of technology, such as encryption, to protect data and information.
- For small organizations or those with a small budget (such as non-profits), consider moving to reputable cloud-based data management platforms, which effectively allows the organization to outsource data security to such platform providers.
- Consider cybersecurity insurance.

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232