Simpson Thacher

Memorandum

Target Settles Consumer Class Action Over Data Breach: A Look Back At the Case Highlights Important Lessons

April 24, 2015

On March 19, 2015, a federal judge in the District of Minnesota preliminarily approved a settlement between Target Corporation and a putative class of consumers in a litigation arising from the breach of Target's computer network in late 2013, scheduling a final approval hearing for November 10, 2015.[1] Under the settlement agreement, Target will pay $10 million to consumers "whose credit or debit card information and/or whose personal information was compromised as a result of the data breach" (the "settlement class").[2]

Pursuant to the settlement, settlement class members who used a credit or debit card at any U.S. Target store between November 27 and December 18, 2013 or who have received notice or otherwise believe that their personal information was compromised as a result of the breach will be eligible for reimbursement up to a maximum of $10,000 if they submit a claim form and "documentary evidence of losses" caused by the

[1] *See* Order Certifying A Settlement Class, Preliminarily Approving Class Action Settlement and Directing Notice to the Settlement Class, *In re Target Corp. Consumer Data Security Breach Litig.*, MDL No. 14-2522 (D. Minn. Mar. 19, 2015) (Dkt. 364). Notably, the settlement agreement is unrelated to the putative class action litigation brought against Target by financial institutions that issue debit and credit cards claiming to have "suffered substantial losses" as a result of Target's alleged "failure to adequately protect its sensitive payment data." Consolidated Class Action Complaint, Financial Institutions Cases, *In re Target Corporation Customer Data Security Breach Litigation (Financial Institutions Cases)*, MDL No. 14-2522 (D. Minn. Aug. 1, 2014) (Dkt. 163). With regard to the financial institutions litigation, Target announced on April 15, 2015 that it reached a settlement with MasterCard, under which Target will pay up to $19 million in recovery payments to MasterCard and its issuing banks. *See* Wall Street Journal, "Target Reaches $19 Million Settlement with MasterCard Over Data Breach" (Apr. 15, 2015).

[2] *Id.* at 2. A portion of the $10 million settlement fund will also be used to make any service payments to the settlement representatives that the court may award. Settlement Agreement and Release at 17, *In re Target Corporation Customer Data Security Breach Litig.*, MDL No. 14-2522 (D. Minn. Mar. 18, 2015) (Dkt. 358-1).

breach, such as credit card statements, invoices, and receipts.[3] Valid losses for which settlement class members can recover include unauthorized, unreimbursed charges on their credit or debit card, time spent addressing unauthorized charges, and other costs or unreimbursed expenses resulting from Target's data breach.[4]

In addition to the $10 million settlement payment, Target will pay expenses associated with the administration of the benefit distribution plan, including the settlement administrator's fees, and any attorneys' fees and expenses awarded by the court to counsel for the settlement class, which will not exceed $6.75 million.

Finally, Target has agreed to implement and maintain specified data security measures as part of the settlement. Target will:

- appoint a compliance officer;
- appoint a Chief Information Security Officer to head its security program;
- maintain a comprehensive, written information security program;
- implement and "[m]aintain a process to monitor for information security events and to respond to such events determined to present a threat"; and
- educate and train employees regarding the security of consumers' personally identifiable information.[5]

Target has agreed to maintain these measures for five years.

While the consumer action was settled before the plaintiffs' allegations could be adjudicated – and without any admissions of wrongdoing or liability – the culmination of the action presents an important opportunity to:

- understand how a data breach can occur and where a company's primary cyber risks may be;
- identify the practical steps companies can and should take to attempt to prevent a data breach, respond to a breach when it does occur, and mitigate the resulting exposure; and
- appreciate the liability companies may face if they do not adequately prevent a breach.

The remainder of this memo will explain how the Target breach allegedly occurred, how Target allegedly responded to the breach, what claims were brought by the putative class of consumer plaintiffs and how the court adjudicated Target's motion to dismiss. Finally, this memo will provide companies and their counsel with practical tips and takeaways from Target's data breach and the resulting lawsuit.

---

[3] Distribution Plan at 1, *In re Target Corporation Customer Data Security Breach Litig.*, MDL No. 14-2522 (D. Minn. Mar. 18, 2015) (Dkt. 358-1).
[4] *See* Claim Form, *In re Target Corporation Customer Data Security Breach Litig.*, MDL No. 14-2522 (D. Minn. Mar. 18, 2015) (Dkt. 358-1).
[5] Settlement Agreement and Release at 13-14.

I. Background

On December 19, 2013, Target announced that its computer systems were hacked, resulting in the theft of payment card data of approximately 40 million customers who made credit and debit card purchases in Target's U.S. stores between November 27 and December 15, 2013.[6] On January 10, 2014, Target issued a press release, noting that in the course of its "ongoing forensic investigation," it had uncovered that "separate from the payment card data previously disclosed," names, mailing addresses, phone numbers or email addresses of up to 70 million customers had also been stolen.[7]

II. The Breach: How It Allegedly Happened

According to the first amended consolidated class action complaint filed against Target by the consumer plaintiffs (the "complaint"), the Target breach had seven distinct phases, together comprising what has been coined by Lockheed Martin as a "kill chain." The complaint notes that because hackers must proceed through all seven steps to plan and execute their attack, "a company has seven different chances along the kill chain to prevent the attack from occurring."[8] Accordingly, it is crucial that corporate management understand and consider each of the links in the "kill chain" – *i.e.*, each of the company's potential vulnerabilities – in order to construct a thoughtful and comprehensive cybersecurity plan.

- **Kill Chain 1st Link – Reconnaissance (June 2013-August 2013).** Hackers in Eastern Europe allegedly "began probing the computer networks of various major U.S. retailers, including Target" and "were searching for loose portals that would allow them access into the retailer's corporate computer systems."[9] The hackers allegedly reached one of Target's third-party vendors, Fazio Mechanical Services, which worked as a heating and air conditioning subcontractor at certain Target stores. Given its work for Target, Fazio had allegedly been provided "limited network credentials by Target, which allowed Fazio virtual access to certain parts of Target's computer network" for purposes of electronic billing, contract submission and project management.[10]
- **Kill Chain 2nd Link – Weaponization (September 2013).** According to the complaint, the hackers stole the credentials to Target's computer network from Fazio in September 2013 by sending a malware program to Fazio in an email. During the same time, it is alleged that "numerous members of Target's security staff raised concerns about what they considered to be vulnerabilities in Target's payment card system," but that those warnings were disregarded.[11]

---

[6] *See* Target Press Release, "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores" (Dec. 19, 2013).
[7] Target Press Release, "Target Provides Update on Data Breach and Financial Performance" (Jan. 10, 2014).
[8] Consumer Plaintiffs' First Amended Consolidated Class Action Complaint at 56, *In re Target Corp. Consumer Data Security Breach Litig.*, MDL No. 14-2522 (D. Minn. Dec. 1, 2014) (Dkt. 258) (hereinafter "Complaint").
[9] *Id.* at 58.
[10] *Id.*
[11] *Id.* at 59-60.

- **Kill Chain 3rd Link – Delivery (November 15 – December 17, 2013).** The hackers allegedly logged onto Target's computer network on November 15, 2013, using the credentials they stole from Fazio. Rather than only accessing the billing, contract submission, and project management portions of Target's computer network, however, the hackers were able to access "the most sensitive part of Target's computer system – its customer payments and personal data network" – because allegedly, the network "was not properly segmented."[12] According to the complaint, the hackers then uploaded their malware onto a small number of Target cash registers as a test, and on November 30, 2013, they "installed their data-stealing malware into a majority of Target's in-store cash registers via remote upload over the Target network."[13] This malware allegedly captured the credit or debit card number and other sensitive personal information of shoppers who swiped their cards at Target store cash registers.
- **Kill Chain 4th and 5th Links – Exploitation and Installation (November 30, 2013).** "Also on or about November 30, 2013, the hackers [allegedly] installed exfiltration malware – a program that takes the stolen information and moves it from Target's computer systems to the hackers' computer systems after several days."[14] The plaintiffs alleged that although Target's security software provider, FireEye, and Target's antivirus system both detected and alerted Target's security personnel to the malware on November 30, "Target's security team took no action."[15] Target allegedly received an identical alert from FireEye on December 2, 2013, but again failed to respond.
- **Kill Chain 6th and 7th Links – Command and Control, Actions on Objectives (December 2-17, 2013).** Having installed malware on Target's cash registers and extractions software on Target's servers, the hackers allegedly collected customers' card data each time a card was swiped at a Target store. This process allegedly continued for a period of almost two weeks – from December 2-15, 2013. According to the complaint, the stolen data was automatically transferred to one of three "secret places installed on the *Target computer network* where the hackers temporarily stored the data before sending it offshore," in order to avoid setting off any internal alarms. "After six days, the data was [allegedly] laundered through a variety of sham computer servers, eventually ending up at its final destination – a server in Russia belonging to the hackers."[16] According to the complaint, on December 11, 2013, an individual associated with Target detected the malware and submitted it to "a company that produces reports about suspicious files submitted by users," but Target allegedly failed to take action.[17] Similarly, the complaint asserts that the following day, "the U.S. Justice Department contacted Target about the breach," but that "Target took three days to try and confirm the veracity of the U.S. officials' statements, thereby allowing the data breach to continue for an additional three days."[18] Target allegedly began removing the malware from its

[12] *Id.* at 60.
[13] *Id.* at 61.
[14] *Id.* at 61-62.
[15] *Id.* at 62.
[16] *Id.* at 63.
[17] *Id.* at 64.
[18] *Id.* at 65-66.

computer network on December 15, suspending "most of the hackers' ability to collect customer billing and personal information."[19] Nonetheless, as Target disclosed in its annual report filing (Form 10-K) of February 1, 2014, additional payment card data was stolen on December 16 and 17, before Target disabled the malware entirely.

III. Target's Alleged Post-Breach Response

The complaint alleges that while Target learned of the breach no later than December 12, 2013, Target did not notify the public of the "massive breach of millions of credit and debit cards that were already flooding the black market" until seven days later.[20] When it did disclose the breach on December 19, 2013, Target allegedly downplayed its significance, asserting that there was "no indication that debit card PINs were impacted"; on December 27, 2013, however, Target disclosed that PIN data was, in fact, removed from Target's systems.[21]

Additionally, on January 10, 2014, Target announced that up to 110 million people were impacted by the breach – not 40 million, as originally disclosed – and that the stolen data also included names, mailing addresses, phone numbers, and email addresses of customers who did not necessarily use their debit or credit cards at Target during the November-December 2013 time frame. According to the complaint, this illustrates "that Target had improperly retained customer data (potentially for many months) that the hackers also extracted as a result of the breach," in violation of Minnesota law and the Payment Card Industry Data Security Standards (information security requirements promulgated by the Payment Card Industry Security Standards Council).[22]

IV. The Claims Brought Against Target

The lawsuit against Target was brought by a group of consumers, "on behalf of themselves and all similarly situated consumers whose account and/or personally identifying information was stolen as a result of the Target data breach," who claimed that they were harmed by the breach.[23] Specifically, the plaintiffs alleged that "Target's conduct – failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' financial account and personal data, and failing to provide timely and adequate notice of the Target data breach" – caused them substantial harm.[24] The injuries they alleged – which, as discussed further below, were found by the court to be sufficient to plead actual injury – include:

- unauthorized charges on their debit/credit card accounts;

---

[19] *Id.* at 66.
[20] *Id.*
[21] *Id.* at 67-68.
[22] *Id.* at 69.
[23] *Id.* at 9.
[24] *Id.* at 1.

- theft of their personal and financial information;
- costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- loss of use of and access to their account funds and related costs for which the plaintiffs were not reimbursed, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- costs associated with time spent to address and attempt to mitigate the actual and future consequences of the data breach, including searching for fraudulent charges and cancelling and reissuing cards;
- "the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit card and personal information being placed in the hands of criminals and already misused via the sale of" their information on the Internet's black market for debit/credit cards;
- "damages to and diminution in value of their personal and financial information entrusted to Target" with the "mutual understanding that Target would safeguard" their data;
- "money paid for products purchased at Target stores," since the plaintiffs "would not have shopped at Target had Target disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information and had Target provided timely and accurate notice of the Target data breach";
- overpayments for products bought at Target, since a portion of the purchase price was for Target's provision of protective security measures, which it did not provide; and
- "continued risk to their financial and personal information, which remains in the possession of Target and which is subject to further breaches so long as Target fails to undertake appropriate and adequate measures to protect" their data in its possession.[25]

Accordingly, the consumer plaintiffs asserted the following claims against Target:

- **Violations of state consumer laws.** The plaintiffs alleged that "Target's failure to maintain adequate computer systems and data security practices to safeguard customers' personal and financial information," Target's failure to disclose these inadequacies, Target's failure to disclose the breach in a timely manner, and Target's continued acceptance of credit and debit card payments "after Target knew or should have known of the data breach and before it purged its systems of the hackers' malware, constitutes unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices" in violation of various state consumer statutes.[26]
- **Violations of state data breach notification statutes.** According to the complaint, Target failed to

[25] *Id.* at 7-9.
[26] *Id.* at 92.

provide timely and accurate notice of the breach when it "knew or reasonably believed such information had been compromised," thereby violating various state statutes that generally require those conducting business in the state and owning or licensing computerized data including personal information to disclose a breach to residents of the state who were affected thereby and that it provide such notice "in the most expedient time possible and without unreasonable delay."[27]

- **Negligence.** Plaintiffs asserted that Target owed them a duty "to exercise reasonable care in obtaining, retaining, securing, safeguarding and protecting their personal and financial information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons."[28] Plaintiffs further alleged that Target owed them a duty "to timely and accurately disclose" that the plaintiffs' "personal and financial information had been or was reasonably believed to have been compromised."[29] The plaintiffs claimed that Target breached these duties.
- **Breach of implied contract.** Plaintiffs asserted that when they "provided their financial and personal information to Target in order to make purchases at Target stores," they "entered into implied contracts with Target pursuant to which Target agreed to safeguard and protect such information and to timely and accurately notify" them that their data had been compromised.[30] Plaintiffs claimed that Target breached these implied contracts.
- **Breach of REDcard agreements.** Target issued branded debit cards, known as Target REDcard debit cards, which were subject to a Target Debit Card Agreement. That agreement incorporated Target's Debit Card Privacy Policy, which states: "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[31] Plaintiffs alleged that each purchase made with a Target REDcard debit card was subject to the terms of the Target Debit Card Agreement and the Target Debit Card Privacy Policy and that Target breached both, as it "did not protect its customers' personal information from unauthorized access and use" and "did not use measures, including computer safeguards and secured files and buildings, to protect" the consumer plaintiffs' personal information from unauthorized access and use.[32]
- **Bailment.** The plaintiffs alleged that when they delivered their personal and financial information to Target, they "intended and understood that Target would adequately safeguard their personal and financial information," and that Target likewise understood this expectation when it accepted possession of the sensitive information.[33] The plaintiffs claimed that as a result, "a bailment (or deposit) was

[27] *Id.* at 102, 105.
[28] *Id.* at 108.
[29] *Id.* at 109.
[30] *Id.* at 114.
[31] *Id.* at 116.
[32] *Id.*
[33] *Id.* at 117-18.

established for the mutual benefit of the parties."[34] According to the plaintiffs, during the bailment, Target owed them a duty "to exercise reasonable care, diligence and prudence in protecting their personal and financial information," but that Target breached that duty "by failing to take appropriate measures to safeguard" the plaintiffs' personal and financial information and "by failing to timely and accurately notify them that their information had been compromised."[35]

- **Unjust enrichment.** According to the complaint, the plaintiffs "conferred a monetary benefit on Target in the form of monies paid for the purchase of goods from Target during the period of the Target data breach," and Target was supposed to use a portion of those monies to pay for the costs of "providing reasonable data security and protection" to the consumer plaintiffs.[36] The plaintiffs alleged, however, that Target failed to reasonably protect their personal and financial information and that as a result, they overpaid for the goods they bought at Target with their credit and debit cards. Similarly, the plaintiffs alleged that they paid for products that they would not have purchased had Target disclosed that it lacked adequate security measures to protect their data and had Target timely and accurately notified them of the breach. The plaintiffs argued that it would be inequitable for Target to be permitted to retain the profits and overcharges it derived from its failure to provide adequate security and should, therefore, be required to disgorge these profits.

V. The Motion to Dismiss

Target filed a motion to dismiss all claims, which the court granted in part and denied in part on December 18, 2014. As a threshold matter, the court addressed Target's "primary argument" – that "Plaintiffs do not have standing to raise any of their claims because Plaintiffs cannot establish injury."[37] The court disagreed, noting that the complaint recites "many of the individual named Plaintiffs' injuries, including unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees."[38] The court held that these allegations are sufficient at the motion to dismiss stage to plead standing. This decision is notable in that it departed from many other rulings in recent consumer data breach cases, which have held that consumer plaintiffs did not adequately allege actual injury and thus did not have standing to sue. The Target ruling suggests that, at least in some jurisdictions, consumer data breach actions may be a more serious threat than previously thought.

The court then turned to the specific claims in the complaint.

- **Violations of state consumer laws.** The court granted in part and denied in part Target's motion to dismiss these statutory claims. The court found that "Plaintiffs have pled economic injury, in the form of

[34] *Id.* at 118.
[35] *Id.*
[36] *Id.* at 119.
[37] *In re Target Corporation Consumer Data Security Breach Litigation*, MDL No. 14-2522, 2014 WL 7192478, at *2 (D. Minn. Dec. 18, 2014).
[38] *Id.*

unreimbursed late fees, new card fees, and other charges" and thus adequately stated a claim even with regard to those state statutes requiring "pecuniary loss."[39] However, the court dismissed the plaintiffs' claims under three state statutes that do not provide a private right of action and held that consumer protection laws in another nine states do not allow class-action treatment of claims brought under those laws.

- **Violations of state data breach notification statutes.** The court also rejected Target's argument that the plaintiffs failed to plead damages resulting from Target's alleged delayed notification of the breach, holding that the plaintiffs adequately pled damages due to their assertion that they "would not have shopped" at the retailer if they had been adequately and timely notified of the breach. The court found that the plaintiffs have "plausibly alleged data-breach notice claims from 26 states," but dismissed the plaintiffs' claims under 12 state data breach statutes, which the plaintiffs conceded or the court found do not provide a private right of action.[40]
- **Negligence.** The court similarly granted in part and denied in part Target's motion to dismiss the plaintiffs' negligence claims. The court again rejected Target's argument that the plaintiffs failed to allege damages resulting from its alleged breaches of duty. The court held, however, that the economic loss rule, which prevents a plaintiff from "recovering for purely economic losses under a tort theory of negligence," serves to bar the plaintiffs' negligence claim in five states.[41] The court allowed the remainder of the negligence claims to stand.
- **Breach of implied contract.** The court found that the plaintiffs sufficiently pled their implied contract claim, plausibly alleging the existence of an implied contract and the terms thereof. The court noted that "a determination of the terms of the alleged implied contract is a factual question" for the jury.[42]
- **Breach of REDcard agreements.** The court dismissed the plaintiffs' breach of contract claim without prejudice. The court opined that if the REDcard agreement was breached due to Target's alleged failure to comply with federal law, the plaintiffs "must plead the federal law or laws with which Target allegedly did not comply."[43] The court provided the plaintiffs the opportunity to re-plead the claim.
- **Bailment.** The court dismissed the plaintiffs' bailment claim with prejudice, finding that the plaintiffs could not plausibly allege the existence of a bailment. The court explained that a bailment is the delivery of property that is later "redelivered to the bailor or otherwise dealt with according to his directions."[44] The court held that even if intangible property such as the plaintiffs' personal financial information "can constitute property subject to bailment principles, [the plaintiffs] have not – and cannot – allege that they

[39] *Id.* at *5.
[40] *Id.* at *14.
[41] *Id.* at *15 (citation and quotations omitted).
[42] *Id.* at *21.
[43] *Id.*
[44] *Id.* (citation and quotations omitted).

and Target agreed that Target would return the property to them."[45] Furthermore, the court noted that the plaintiffs alleged "that third parties stole the information, not that Target wrongfully retained that information."[46]

- **Unjust enrichment.** The court allowed the plaintiffs' unjust enrichment claim to proceed under one of the plaintiffs' two theories – that "had Target notified its customers about the data breach in a timely manner, Plaintiffs would not have shopped at Target and thus any money Plaintiffs spent at Target after Target knew or should have known about the breach is money to which Target is not entitled."[47] However, the court dismissed the unjust enrichment claim based on the plaintiffs' other theory – namely, that the plaintiffs were overcharged for the goods they purchased at Target because the purchase price included the cost of adequate data security, which Target allegedly did not deliver. The court reasoned that because Target charges all its customers the same prices, regardless of whether they are paying with cash or a debit/credit card, despite the fact that cash customers are not at risk of their financial information being stolen, the plaintiffs' "overcharge theory" is "implausible."[48]

VI. Lessons Learned From *Target* and Other Recent Data Breach Cases

Although the *Target* case was not adjudicated on the merits, it sheds some light on companies' exposure to cyber risk, how companies might be able to mitigate this exposure and/or prevent a data breach, and how they should respond when a data breach does occur.

A. Cyber Risks

In order to take effective steps toward preventing a data breach, a company must first understand its top cyber risks. Among others, these risks may include:

- outside attacks and misuse by current and departing employees;
- "social engineering" to gain network access from users with "privileged access" ("social engineering" refers to psychological manipulation of people into performing actions or divulging confidential information, often in violation of security policies);
- lost/stolen devices that are not properly protected with encryption and/or remote management;
- inadequate client, customer and employee data protection;
- use of data in violation of U.S. or foreign laws or directives;
- server vulnerabilities and/or laptop and personal computer vulnerabilities;
- cloud computing;

---

[45] *Id.*
[46] *Id.*
[47] *Id.* at *22.
[48] *Id.*

- outsourcing, vendor and/or service provider risks;
- failure to address privacy/cybersecurity in initial design phase of new products and in any system upgrades or major changes; and
- inadequate authentication procedures for customers and users.

B. Preventing and Preparing for a Data Breach

- **Leadership.** As a threshold matter, companies should ensure that they have a senior person with clear responsibility for organization-wide security preparedness and with support from the top.
- **Budget and Staffing.** Corporate management should ensure that it has allocated an appropriate portion of the budget and adequate staff to cyber risk management. In addition, within the overall cyber budget, the allocation of funds should be prioritized in accordance with relative risk.
- **Written Cybersecurity Plan.** Corporate management should devise a comprehensive, written privacy/cybersecurity plan, which should be reviewed by and distributed to all those who may be involved in its execution. In creating this plan, some issues corporate management should consider are:
    - what type of data the company collects and where this data resides;
    - whether the company monitors to avoid collecting and storing non-essential customer data;
    - whether and how the company ensures that data is destroyed responsibly after it has outlived its business purpose;
    - whether more sensitive data is stored separately with higher safeguards;
    - how access credentials are selected and allocated within the company (e.g., whether employees are granted access to sensitive data only if necessary for them to perform their job duties);
    - whether the company keeps up-to-date records of and audits who is able to access what data;
    - what measures the company takes to protect against the downloading of malicious data;
    - what procedures for password creation/protection and encryption the company uses for data transmission, storage and access for employees, vendors and customers/users;
    - what additional security measures the company implements and maintains to secure its data;
    - what measures the company takes to reduce the risk that data will be transferred from the company's internal network to the outside internet (e.g., a firewall between the company's internal systems and the internet, blocking particular internet connections known to be used by hackers, and/or creating a list of approved servers to which the company's network is permitted to upload);
    - what the company's protocol is for handling lost laptops and mobile devices;
    - how cybersecurity concerns are addressed for departing employees;

- whether the company monitors its outgoing data transmissions for possible misconduct;
- what market practice is among companies in the same industry; and
- whether it is important for the company to engage third parties to test its cybersecurity preparedness and/or whether the company has performed other security and privacy audits.

The company's data security program should be reviewed at least annually.

- **Employee Training and Education.** Companies should institute effective training programs that instruct employees on the appropriate handling and protection of sensitive data. As is always the case, the employee training programs put in place should be meaningful and should consist of more than written policies. Among other things, employee training should:
  - stress the importance of common sense protective measures, such as not sharing passwords, using strong/complex passwords, changing passwords frequently, not using the same password for all accounts, locking or shutting down computers when they are not in use, removing any unnecessary programs from computers, not opening emails from unknown sources, refraining from downloading unapproved software, and maintaining the physical security of mobile and data storage devices;
  - teach employees not to reveal sensitive information over the phone or in person unless the employee is certain of the other individual's identity; and
  - educate relevant personnel on procedures for responding to data security concerns raised by employees and to alerts from the company's security software tools or antivirus systems.

  Companies should institute audit practices to assess employee compliance with their data protection policies.
- **Third-Party Vendors.** Companies should take steps to mitigate the cybersecurity risks associated with outsourcing business functions to third parties. These risks can be significant; according to one study, 63% of data breaches were linked to third parties.[49] Steps companies could take to mitigate these risks include:
  - limiting the amount of publicly available information regarding third-party vendors and requiring, to the extent possible, that such vendors be similarly discreet;
  - ensuring that third-party vendors are aware of the company's information security policies and agree to adhere to them;
  - restricting access of third parties only to the servers/information they need in order to do their job;
  - ensuring that third-party vendors properly handle and secure shared sensitive information, e.g., by reviewing vendors' security policies (such as those pertaining to employee background screenings

[49] Trustwave 2013 Global Security Report at 2.

and data management) and defining data security standards and expectations with third-party vendors (such as requiring monitoring of their networks' integrity and specifying anti-malware software);

- ensuring that agreements with third parties clearly identify whether and how the service provider will safeguard the organization's sensitive data and whether the service provider will notify the organization in case of a breach;
- ensuring that agreements with third-party vendors address whether any services will be subcontracted to other vendors and, if so, requiring minimum data security standards and expectations to be set;
- requiring two-factor authentication for vendors to access the company's network, which would include "a regular password system . . . augmented by a second step, such as providing a code sent to the vendor's mobile phone or answering extra security questions"[50]; and
- ensuring proper segmentation between the parts of the network accessible to vendors and those that house payment or other sensitive data to which the vendors do not need access.

- **Legal Compliance and Regulatory.** Companies should:
  - ensure that their relevant employees have an effective system in place for staying abreast of and complying with evolving federal, state, and international data security laws and regulations that are applicable to the company's business operations (including, for example, laws that restrict companies from retaining the debit/credit card's security code data, PIN verification code, and/or the contents of the card's magnetic stripe data following the authorization of the transaction), as well as industry technical standards and best practices on information security; and
  - where appropriate, establish relationships with local and national authorities responsible for cyber-crime prevention and response (*e.g.*, the Federal Bureau of Investigation).
- **Insurance.** Companies should consider purchasing cyber liability insurance, which often covers forensic investigations of a breach, notification of affected individuals, payments to customers who have lost confidential information, credit monitoring for affected individuals, regulatory compliance measures, the hiring of public relations consultants, and lawsuit defense and indemnification.
- **Detection.** Companies must ensure that they have state-of-the-art technology for preventing the downloading of malicious software and detecting and alerting the company to attempted breaches.
- **Comprehensive, Written Breach Response Plan.** It is critical that companies be prepared to respond to a breach quickly, efficiently and calmly. To that end, companies should:
  - form a breach response team composed of individuals from key departments (including legal,

[50] Complaint at 61.

corporate communications, and information technology security) and identify individual functions and responsibilities in case of a breach;

- select an individual with ultimate responsibility for overall implementation of the plan, as well as individuals who will periodically review and update the plan;
- identify outside advisors that may need to be contacted in the event of a breach, such as legal, forensic, and public relations specialists, as well as regulators and law enforcement authorities;
- consider having standing contracts in place with such outside experts so that, in the event of a breach, time does not need to be spent on contract negotiation;
- outline each phase of their incident response plan, from initial response activities (such as reporting the breach) to strategies for notifying affected parties, to breach response review and the remediation process;
- create hypothetical scenarios to test the plan; and
- ensure that the plan is reviewed regularly and revised as necessary.

C. Responding to a Data Breach

- **Validate the Breach.** Upon suspecting a breach, a company should immediately examine any initial information, available logs and, if possible, the type of information disclosed and/or the method of disclosure in order to confirm that an actual breach has occurred. Once the breach is confirmed, the company should determine the scope of the breach and those affected. Because of the risk of evidence contamination, the company's internal staff should be careful not to disturb the servers; accordingly, once the breach is confirmed, a forensic expert may need to be consulted in order to evaluate the breach.
- **Stop the Breach.** Upon confirming the breach and its scope, a company must take immediate action to stop the breach (if it is still underway) and rectify any vulnerabilities in the system. The company should work with a forensics firm or qualified Computer Emergency Response Team ("CERT") members to identify the systems impacted, the compromised data, and the malware or malicious files. The forensics team will make a determination as to when it is best to delete malware or malicious files without compromising evidence. Additionally, the forensics team will determine if the compromised system(s) should be taken "off-line," shut down, or isolated from the rest of the network. The company should ensure that it removes the malware, such that the cyber-attack cannot continue, and that it assesses and corrects – perhaps with the help of consultants – the vulnerabilities within the system that enabled the breach.
- **Follow the Company's Data Breach Response Plan.** Immediately upon discovering the breach, the company should assemble its selected incident response team and begin its investigation pursuant to its breach response plan. It is often worthwhile to conduct the investigation in consultation with counsel, as this will facilitate compliance with potentially complex legal obligations and will make it more likely

that certain communications will be protected by privilege in any potential legal action. In addition, the company should give serious consideration to whether and when it should self-report the breach to the relevant law enforcement authorities. Finally, throughout the investigation, the company should monitor information sources – particularly the news media – in order to understand how the media is reacting and determine whether and/or how to adjust the company's response.

- **Notify Customers.** It is imperative that the company and its legal department understand and comply with any applicable state, federal, or internationally imposed legal mandates governing the timing and/or content of customer notification. As a general matter, however, companies should notify customers of the breach as soon as possible after the breach is validated and its scope is understood. Customers should be notified through more than one channel, such as by email, postal mail, and press release. With regard to the content of the customer notification, the company should:
  - clearly state, to the extent known, the "who, what, when, where, and how" of the breach;
  - ensure that all the information provided is accurate;
  - ensure that the notification does not omit any key details or mislead recipients in its presentation;
  - avoid absolutes, such as absolute statements about the breadth or depth of the breach, as this could change quickly;
  - empathize with customers and reassure them that they are being protected;
  - offer timetables of what will happen next in the investigation;
  - provide recommended steps customers should take to protect personal information;
  - explain the steps the company has taken and/or plans to take to address the issue; and
  - mention, where applicable, that the company is cooperating with legal authorities
- **Provide Customer Support.** A company that has experienced a data breach should support its customers, for example, by providing information phone lines, credit monitoring, or investigator or identity restoration services. The company could also use its corporate website and/or might consider purchasing keywords on popular internet search engines to direct potentially affected customers to helpful post-breach information.
- **Issue a Press Release, Where Appropriate.** Where the company determines that a press release is appropriate, it should issue the release in a timely manner – as soon as possible after or in conjunction with its notification to affected individuals. Like its other forms of customer notification, the company's press release should be transparent, and it should state how customers are being notified, contain the extent and content of the notification, and describe the steps being taken to rectify the situation. In drafting the press release, companies should be mindful of what they do not yet know about the breach. In addition, the press release should reflect that the company is taking ownership of the breach, rather

than "playing the victim." Finally, it is advisable that key departments (including legal and information technology security) review the press release prior to its dissemination.

- **Ensure Legal Compliance.** The company should consult with legal counsel at all stages of responding to a breach to ensure that the company is complying with any applicable state, federal, and international laws.
- **Determine Whether to Engage External Consultants.** The company should assess whether and when it should hire consultants, such as forensic specialists or a public relations firm, to assist in the company's investigation or to help the company navigate the aftermath of the breach. The company should consider having its external consultants supervised by counsel so as to increase the likelihood that certain communications between the company and consultants will be covered by the attorney-client privilege.
- **Review Insurance Coverage Policies.** The company should determine the extent to which it is covered for the data breach.
- **Assess the Breach Response Plan.** During and after the investigation and the company's response process, the company should assess the effectiveness of its response to the data breach and modify its breach response plan accordingly.

If you have any questions or would like additional information, please do not hesitate to contact any member of the Firm's Data Privacy and Cybersecurity Practice.

Simpson Thacher Worldwide

UNITED STATES

New York
425 Lexington Avenue
New York, NY 10017
+1-212-455-2000

Houston
2 Houston Center
909 Fannin Street
Houston, TX 77010
+1-713-821-5650

Los Angeles
1999 Avenue of the Stars
Los Angeles, CA 90067
+1-310-407-7500

Palo Alto
2475 Hanover Street
Palo Alto, CA 94304
+1-650-251-5000

Washington, D.C.
1155 F Street, N.W.
Washington, D.C. 20004
+1-202-636-5500

EUROPE

London
CityPoint
One Ropemaker Street
London EC2Y 9HU
England
+44-(0)20-7275-6500

ASIA

Beijing
3919 China World Tower
1 Jian Guo Men Wai Avenue
Beijing 100004
China
+86-10-5965-2999

Hong Kong
ICBC Tower
3 Garden Road, Central
Hong Kong
+852-2514-7600

Seoul
West Tower, Mirae Asset Center 1
26 Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
+82-2-6030-3800

Tokyo
Ark Hills Sengokuyama Mori Tower
9-10, Roppongi 1-Chome
Minato-Ku, Tokyo 106-0032
Japan
+81-3-5562-6200

SOUTH AMERICA

São Paulo
Av. Presidente Juscelino Kubitschek, 1455
São Paulo, SP 04543-011
Brazil
+55-11-3546-1000