HARVARD | BUSINESS | SCHOOL

9-117-027

REV: JANUARY 10, 2019

SURAJ SRINIVASAN

LYNN PAINE

NEERAJ GOYAL

Cyber Breach at Target

In November 2013, Target Corporation was the subject of one of the largest cyberattacks in history. Heading into Christmas, the retail industry's busiest season of the year, hackers stole credit and debit card information for 40 million Target customers and names, as well as home and email addresses for another 70 million. The attack and Target's response exposed the company to intense criticism and raised questions about the accountability of Target's board of directors and the Audit Committee and Corporate Responsibility Committee that were responsible for the oversight of both operational and reputational risks. Leading proxy advisory firm Institutional Shareholder Services (ISS) recommended that Target shareholders vote against the re-election of 7 of Target's 10 board members, including the chair of the Audit Committee. Investors filed derivative suits charging the board with breach of fiduciary duty and waste of corporate assets, with lack of diligence in protecting sensitive customer information, and with failure to oversee risks to brand value. While Target's board vigorously defended its performance, observers were left wondering about the extent of board accountability for a breach of such large magnitude.

Company Background

Target's origins could be traced to George Dayton's establishment of a Minneapolis department store in 1902. In 1909, Dayton opened a discount store, focusing on customers who could not afford the higher-priced department store.[1] In the 1950s, discount stores started taking market share from department stores by offering branded, quality products at lower prices. In 1962, the Dayton Company opened its discount stores branded Target at the same time Sam Walton was founding Walmart and Sebastian Kresge was starting Kmart. Target created its unique brand image by selling quality goods at low prices in an upscale environment, when its competitors focused on selling goods as cheaply as possible. In advance of Target's opening, Douglas Dayton had stated in 1961, "[Target will] combine the best of the fashion world with the best of the discount world, a quality store with quality merchandise at discount prices, and a discount supermarket . . . a store you can be proud to shop in, a store you can have confidence in, a store that is fun to shop and exciting to visit."[2]

Target embraced this approach as the store that offered everyday consumers high-quality products at discount store prices embodied in its slogan, "Pay Less, Expect More," first advertised in 1994.[3] This ethos allowed Target to differentiate itself from competitors like Walmart. Target appealed to the latest

Professors Suraj Srinivasan and Lynn Paine and Research Associate Neeraj Goyal prepared this case. This case was developed from published sources. Funding for the development of this case was provided by Harvard Business School and not by the company. HBS cases are developed solely as the basis for class discussion. Cases are not intended to serve as endorsements, sources of primary data, or illustrations of effective or ineffective management.

consumer tastes by offering new fashions and fresh trends and even collaborated with designer labels such as Maternity, Jason Wu, and Liz Lange.[4]

In 2004, the Dayton Company divested its Mervyn's and Marshall Field's stores and focused solely on Target, which accounted for nearly 80% of the sales of the parent company.[5] For fiscal 2013, Target had revenues of over $72 billion, reflecting a 2.8% compound annual growth rate over the previous five years.[6] (See **Exhibits 1–3** for recent financial statements and Target's stock performance.) As of November 2013, Target operated 1,919 stores, 1,797 in the U.S. and 122 in Canada, representing over 254 million retail square feet. Target competed with the largest U.S. retailers, such as Walmart, Sears, and Kohl's.[7,8] Target was proud of its corporate citizenship. Every financial press release in 2013 included this statement: "Since 1946, Target has given 5 percent of its profit through community grants and programs; today, that giving equals more than $4 million a week."[9]

A typical Target store had around 80,000 Stock Keeping Units (SKU)[a] offering a wide variety of electronics, household products, apparel, and even groceries at its SuperTarget locations.[10] Target also offered its customers credit through its REDcard program. As with all retailers, the Thanksgiving-to-Christmas shopping season represented the busiest period for Target; for the 2013 Christmas season, the company had increased employment by 50,000 over its normal base of around 366,000.[11,12] In each year from 2010–2013, the company derived around 30% of its revenues from the fourth quarter.[13]

Hackers Strike Target

In September 2013, hackers from an unknown location initiated a phishing email campaign[b] against one of Target's external heating and ventilation providers, Fazio Mechanical Services.[14,15] Information about Target's vendors was publicly available online and hence accessible to anyone looking for it. When a Fazio employee opened the malicious email, it enabled hackers to steal all of Fazio's passwords.[16] Fazio's main method to detect malware was a free version of a security product called "Malwarebytes Anti-Malware," whose license explicitly prohibited corporate use. But Fazio had used it anyway, and Target did not monitor the vendor's security arrangements. Also, that same month, Target's security team identified vulnerabilities in the firm's payment card systems and cash registers, but no further investigations were undertaken or ordered by Target officials.[17]

On November 15, 2013, using Fazio's credentials, hackers gained access to Target's network for electronic billing, project management, and contract submission.[18] To prevent such an intrusion, Target could have required two-factor authentication—a regular password, enhanced with a verification code sent to the vendor's mobile phone—which was a payment card industry (PCI) standard for remote access by third parties, but was not being required by Target.[19,20] According to an industry analyst who managed some of Target's vendor relationships:[21]

> Only the vendors in the highest security group—those required to directly access confidential information—would be given a token, and instructions on how to access that portion of the network. . . . Target would have paid very little attention to vendors like

[a] An SKU identifies each distinct item offered in a retailer's product catalog, and can vary by manufacturer, material, size, color, and other features.

[b] Phishing email campaigns are attempts by Internet scammers to acquire sensitive personal information such as user names and passwords, credit card information, and other data by sending emails with malicious links. These emails typically ask unsuspecting users to visit a fraudulent website and enter information into a seemingly appropriate website, but allow scammers to steal and misuse gathered data.

> Fazio, and I would be surprised if there was ever even a basic security assessment done of those types of vendors by Target.

Moreover, because Target's network was not properly segmented, the hackers gained access to sensitive customer payments and personal data.[22] According to an industry expert, "there should never be a route between a network for an outside contractor (such as Fazio) and the network for payment data. In Target's case, there was and the hackers found it and exploited it."[23]

According to investigators, the attack started on a small number of Point-of-Sale (POS) systems between November 15 and November 28, heading into the busiest holiday shopping season for U.S. retailers. By November 30, the majority of Target's POS system had been affected. The hackers installed malware[c] called "Citadel" on specific POS systems in Target's retail stores.[24,25] Once the hackers installed the malware, they used a "RAM scraping" attack method;[d] this allowed the hackers to collect encrypted data as it passed from the POS systems to the payment processing providers Visa and MasterCard.[26] The malware collected credit and debit card information encrypted on the cards' magnetic strips whenever a customer swiped at the store.[27]

Target's network design allowed hackers to move about Target's internal networks and even update the malware for another wave of attacks.[28] According to a security report, "The attackers reportedly first installed three variants of this malware on November 30 and updated it twice more, just before midnight on December 2 and just after midnight on December 3."[29] On December 2, and over the next two weeks, the malware started exporting the collected data through another compromised Target server, to an external server based in Russia.[30] (Refer to **Exhibit 4** for a timeline of the cyberattack.)

In all, hackers gathered 11 gigabytes (GB) of stolen data, which represented around 40 million debit and credit card accounts[e] and could be sold on the black market for as much as $100 per credit/debit card number.[31,32,33] According to lawsuits filed by affected customers, "On Dec. 11, one week after hackers breached Target's systems, Easy Solutions, a company that tracks fraud, noticed a ten to twentyfold increase in the number of high-value stolen cards on black market web sites, from nearly every bank and credit union."[34]

Security Warnings Initially Ignored

Target contracted its cybersecurity monitoring to FireEye, Inc., a firm that provided malware detection tools and a team of security specialists in Bangalore, India. These security specialists were required to monitor Target's systems around the clock.[35] The FireEye team initially raised an alert of an attack right after the Black Friday[f] shopping season, on November 30.[36,37,38] The FireEye team in India sent an electronic alert to Target's in-house security team in Minnesota indicating that the

---

[c] Malware (or "malicious software") is any program or file that is harmful to a computer user. This includes computer viruses, worms, Trojan horses, and also spyware, programming that gathers information about a computer user without permission.

[d] RAM scraping or memory scraping malware targets encrypted data in a computer system's memory, where the data is in plain-text format. According to security experts, in order to process data or code, the information needs to be decrypted in memory, which makes the system vulnerable. RAM scraping malware intercepts the data when the code sees 16 characters ending with a zero or special character, as is the case with credit card data.

[e] Target later revised its estimates of affected customers from 70 million to 110 million, and included other types of data such as mailing and email addresses and phone numbers, data that Target had collected over time.

[f] Black Friday is the Friday after Thanksgiving Day (Thanksgiving is the fourth Thursday in November), and marks the beginning of the Christmas shopping period in the U.S. In the 2000s, it became increasingly common for U.S. retailers to open earlier in the day at 5 or 6 a.m. on Black Friday, and in 2014, Target opened its doors at 6 p.m. on Thanksgiving Thursday.

monitoring software had detected malware intrusions but that the install had not been activated yet. However, the U.S. team did not respond to the alert. According to the subsequent investigation, the U.S. team could have potentially viewed the FireEye alert as a false positive since multiple alerts were being generated under generic names like "malware.binary."[39]

Once the malware started extracting the data to the hackers on December 2, the security team in India again alerted Target's security team in Minneapolis, but got no response.[40,41] From December 2 through December 15, hackers collected customers' credit card data in real time. Every time a customer swiped a card at the register, the financial data linked to the card was sent to one of three "staging points"—storage facilities created within Target's networks. To avoid setting off alarms, the data was stored on Target's networks for six days and then transmitted through a number of fake servers before being sent to the hackers' personal servers.

According to two experts who audited the breach, "The breach could have been stopped there without human intervention. The system has an option to automatically delete malware as it's detected. . . . Target's security team turned that function off."[42] It was unclear why this function was turned off. (Refer to **Exhibit 5** for a graphical representation of Target's missed opportunities, and **Exhibit 6** for a summary of analysis by a U.S. Senate subcommittee on the Target data breach.)

Before the attack, the information security functions were split among the Chief Financial Officer, the Chief Information Officer, and the General Counsel (refer to **Exhibit 7** for a description of Target's pre-breach information security structure). Beth Jacob was Target's Chief Information Officer (CIO) during the attack, and she oversaw teams in India and the U.S.[43] Although the cyberattack through the POS system was not necessarily under the direct purview of the CIO, according to analysts, detecting the breach seemed to fall under the CIO's responsibilities.[44]

Target Discovers the Breach (week of December 12–19)

On December 12, 2013, the U.S. Department of Justice (DOJ) contacted Target about the breach, making the company's U.S. executive team aware of its seriousness.[45] On the same day, JP Morgan Chase began alerting credit card companies of a pattern of fraudulent credit card charges initiated at Target.[46] The next day, Target executives met with the DOJ and the U.S. Secret Service, and on December 14, Target hired a third-party forensics team to investigate the breach.[47]

In a later interview with CNBC, Target CEO Gregg Steinhafel explained that he first found out about the breach on the morning of December 15 after the internal security team had confirmed the attack. On December 15, Target began removing the malware from its systems and the attackers started losing access to the Target network, but Target wanted to avoid disruption in store operations and did not close its stores.[48] The company took until 6 p.m. on December 15 to remove the malware.[g,49] On the 16th, Target initiated an investigation and began forensic work, and on December 17, the company started preparing its stores and call centers to answer customers' questions.[50]

The first public indication of the breach came on December 18, from *Krebs on Security*, a popular online security blog run by David Krebs.[51,52] Sources at credit card issuers informed Krebs that the breach extended to nearly all Target locations in the U.S. and had occurred from Thanksgiving to December 15. It was unclear if online customers had been affected. Krebs reported that more than one million cards had been compromised, and warned that if hackers were able to steal debit card PIN data,

[g] By December 15, Target removed most of the malware on its networks. However, card information for 56 additional customers who shopped at Target on December 16 and December 17 were stolen since a small number of POS systems that had been disconnected from the network during the initial cleaning continued to be infected until then.

they would potentially be able to steal money directly from customers' accounts and ATMs.[53] Media outlets soon picked up the story and obtained confirmation from the Secret Service that it was investigating the incident. One media outlet quoting an unnamed source stated, "[W]hen all is said and done, this one will put its mark up there with some of the largest retail breaches to date."[54] Target refused to confirm the incident that day.

Target Announces the Breach

On December 19, one week after it was first contacted by the DOJ, Target posted on its corporate website (and not the more frequented consumer website) and distributed through regular media outlets a press release stating that it was "aware of" unauthorized access to payment card data.[55] The press release explained that between November 27 and December 15, 2013, approximately 40 million credit and debit card accounts belonging to Target customers had been affected.[56] "Target alerted authorities and financial institutions immediately after it was made aware of the unauthorized access, and is putting all appropriate resources behind these efforts," stated the press release.[57]

Target customers immediately began noticing fraudulent transactions on their accounts. One customer stated, "Sure enough, there were charges from various online retailers that neither I nor my husband had made."[58] Another customer called Target's hotline "at least 40 times" on December 20, the day after the announcement, and "When she finally got through, the pre-recorded message referred her to a Web address: http . . . forward slash, forward slash . . . and so on." Customers complained about poor service when they tried to gather more information on the breach and how it might affect them.[59] Customers found Target's website difficult to navigate, and the dearth of information left customers ill-equipped to plan.[60]

On December 20, CEO Steinhafel explained in a letter posted on Target's website and sent to customers via email and U.S. mail that "there is no indication that PIN numbers have been compromised."[61,62] The CEO also explained that simply having shopped at Target during this period did not imply that they would be victims of the fraud, and that the level of fraud had been low in similar situations.[63] Target offered free credit and theft monitoring for affected customers for a year and reassured customers that they would not be held liable for any fraudulent charges resulting from the breach.[64] (See **Exhibit 8a** for Target's announcement and **Exhibit 8b** for Steinhafel's letter.) Target also stated that it was not likely that birth dates and Social Security numbers had been accessed.[65]

In a video apology posted on Target's corporate website the same day, Steinhafel explained that the wait times to Target's call centers were "unacceptable" and that his team was "working around the clock" to shorten the wait times. Steinhafel offered the 10% employee discount to customers who would shop in Target stores on December 21 and December 22.[66,67] The CEO highlighted three steps for its concerned customers to follow, namely, to check credit card activity to see if there were any suspicious charges, contact the card provider or Target itself if a customer found suspicious charges, and check their credit services report.[68] However, customers felt ill-equipped to protect themselves. One customer stated, "How the hell am I supposed to monitor my account if I can't get into it. . . . No excuse you have is good enough."[69] The pressure on Target's management to efficiently manage the breach response continued to build.

On December 20, *Krebs on Security* learned that underground black markets had been inundated with stolen credit and debit cards that were being sold in batches of one million cards for $20 to $100 per card.[70] These card batches were considered high "quality," as data had been stolen from the cards' magnetic stripes and could be cloned more easily. Krebs spoke with a bank in New England and found that although bank officials had so far identified 6,000 customers (5% of its card portfolio) who had

shopped at Target during the breach period, they had not received any notifications from Target or law enforcement. The bank representative stated, "Nobody has notified us. Law enforcement hasn't said anything, our statewide banking associations haven't sent anything out . . . nothing."[71]

On December 25, a payment executive familiar with Target's breach stated that PIN information had been stolen, and on December 27, Target reversed its earlier position to confirm that PIN information had, in fact, been stolen.[72,73] In addition to PIN data, CVV numbers and expiration dates had been compromised, and customers need not have even swiped their cards in a Target store. Target had retained data over time, which had now been stolen.[74] Target explained that although PIN information had been stolen, it remained encrypted, and a decryption key, which was necessary to unlock and decipher the PIN code, was not stolen, as it was never stored on Target's network. Only the independent payment processor could decrypt this code.[75]

On January 10, Target announced that, in addition to payment card data, personal information including names and mailing and email addresses had also been stolen for 70 million customers, 30 million more than Target had initially reported.[76,77,78] This revelation raised questions about what other data the hackers might have accessed. An industry analyst explained, "For somebody to actually go out and open credit in your name, it's pretty tough to do if they don't have your Social [Security number]. . . . But if they have your Social and have all this other stuff too, it compounds the problem."[79] Target collected Social Security numbers from customers who applied for Target's flagship credit card product, the REDcard. A brand expert captured the grim customer sentiment:

> The retailer has reached its lowest consumer perception point since at least June 2007. While many say they can understand a store getting hacked, they're having problems getting their heads around what one customer called a "disheartening" response to the security breach. Many are vowing to avoid shopping at Target, while others have canceled their REDcards . . . or are planning to sue.[80]

Steinhafel explained in an interview on January 12, 2014: "The call center experience initially, was unacceptable, and for that, I apologize for that. . . . As of Friday [January 10], our wait times were only 8 seconds."[81]

The hackers targeted a large number of customers, which allowed for small charges that could easily slip past an unsuspecting eye.[82] "It's just very frustrating," explained an affected customer who had pored through her statements in great detail to find two unauthorized charges—one from iTunes, and a strange $14 charge she did not make. Another customer found her bank account depleted from $3,643.53 to $5.86, forcing her to borrow for food and for her son's tuition.[83]

Postmortem: What Went Wrong?

A Senate investigation found that at least two months before these attacks, Target's security team had highlighted vulnerabilities in Target's POS system and asked to review Target's payment network.[84] According to a former employee, Target was updating its payment terminals, and this left security analysts with less time to find flaws in the system. But the Senate report found that the review request was ignored, as Target was preparing for a busy Black Friday weekend. It remained unclear who within Target's management made this decision, but according to an employee:

> The sheer volume of warnings that retailers receive makes it hard to know which to take seriously. Target has an extensive cybersecurity intelligence team, which sees numerous threats each week and could prioritize only so many issues.[85,86]

Target had received a certification of compliance with the Payment Card Industry Data Security Standards (PCI DSS) as recently as September 2013 from Trustwave Holdings, an information security company.[87,88] Card companies required merchants to receive this certification before they would process transactions. In late 2013, the payment card industry was set to adopt the latest set of standards, PCI DSS 3.0. Large organizations such as Target were subject to yearly audits of their security networks.[89] Trustwave was considered a leader in the security industry, having performed thousands of these certifications and audits for retailers and payment processors.[90]

However, some clients certified by Trustwave had suffered large cyberattacks soon after receiving their certifications.[91] According to industry observers, "It [recent cyberattacks] also raised important questions about the liability of third-party companies that audit and certify the trustworthiness of restaurants, retailers and others that accept bank card payments."[92] In addition, the standards themselves were not considered dynamic. According to analysts, security needs evolved at a quicker pace—a compliant company could become non-complying the next month if firewalls were installed and configured incorrectly, or if segregated systems became connected because access restrictions were misappropriated.[93] In addition, new vulnerabilities could arise if a company changed servers or its software architecture, or even installed new programs. As such, industry analysts considered the PCI standards to be a "floor and not the ceiling."[94]

According to a technology industry expert, it was unlikely that Target was even compliant with PCI 2.0 at the time of the breach, because the attack affecting millions of customers went unnoticed for 18 days.[95] To disrupt the attack, Target should have taken measures called for in the PCI DSS 2.1, the version of PCI DSS in effect at the time of the breach. Target should have eliminated unneeded default accounts, which the hackers utilized to access the most sensitive parts of Target's network. Additionally, Target should have required vendors to closely monitor the integrity of their critical system files, which would have put Fazio on notice that hackers had stolen its Target credentials. Finally, Target could have created stronger firewalls between its internal systems and external Internet; checked the location of the credentialed log-ons; and created a list of approved servers and Internet connections Target's network could communicate with.[96,97]

The Aftermath

Target's total sales fell 6.6% for the fourth quarter of 2013, and compared to the previous year, net earnings for the fourth quarter dropped by 46% to $520 million.[98,99] As of February 1, 2014, six weeks after the date of the breach announcement, the firm's stock price was down 8.8% to $56.7 per share.[100] Target also forecasted roughly 20% lower earnings per share (EPS) guidance after the episode. By the end of 2014, Target had incurred $162 million in costs due to the data breach, and the amount was expected to increase as a result of pending litigation.[101,102]

Although Target made a concerted effort to control the damage from the attack, it faced extensive media scrutiny, investigations by Congress, the Securities and Exchange Commission (SEC), the DOJ, and the Federal Trade Commission (FTC), as well as litigation from affected customers, banks, and shareholders.

Congressional Inquiries

Target executives were called to testify about the breach before the Senate Judiciary Committee and the Senate Commerce, Science, and Transportation Committee. The day before the hearing on March 27, the office of Senator John D. Rockefeller IV, Chair of the Commerce, Science, and Transportation Committee, released a report detailing how the breach occurred, and how Target missed numerous

opportunities to stop the attack.[103] (See **Exhibit 6** for a summary of the committee's analysis.) At the hearing, Senator Richard Blumenthal, a committee member stated:

> It [the investigative report] explains how Target could have prevented the breach if you had stopped attackers from completing even just one of the steps [described in the report]. . . . The best technology in the world is useless unless there's good management, and here, to be quite blunt, there were multiple warnings from the company's anti-intrusion software. They were missed by management. . . . If Target failed to adequately protect customer information, it denied customers the protection that they rightly expect when a business collects their personal information. [104,105,106]

Senator Blumenthal continued, "In the future, at some point, the CEO and the board of directors have to take responsibility."[107,108]

Litigation

Target faced lawsuits from individual customers, banks that provided credit card services, and investors. As of May 7, 2014, Target had 81 consumer cases, 28 bank cases, and 4 shareholder cases filed and pending before various courts.[109]

Customer Lawsuits

The hackers picked an opportune time to strike. The Thanksgiving and Christmas shopping season marked one of the largest shopping periods for U.S. consumers. In 2014, over Thanksgiving and the following day (Black Friday) alone, Americans spent over $12 billion, with the bulk of these sales, over $9 billion, coming in on Black Friday.[110]

The track data[h] stolen by the hackers allowed them to counterfeit information encoded in a card's magnetic strip and, with the PIN data, to withdraw money directly from customers' accounts.[111, 112] Had they known that PIN numbers had been compromised, customers could have requested replacement cards and protected themselves. However, until December 27, Target claimed that there was no indication that debit card PINs were affected and maintained that the culprits could not withdraw money from customer accounts. One lawsuit gave the example of one customer, a mother of five children, whose card was declined when she attempted a withdrawal:[113]

> Ms. [Brystal] Keller had a fraudulent charge of $434.15 . . . another in the amount of $276. . . . Ms. Keller's bank did not reimburse either fraudulent charge until January 7, 2014, more than two weeks after the fraud occurred. . . . She was locked out of her account from December 26, 2013 until January 21, 2014. . . . Ms. Keller missed a rent payment, a car loan payment . . . had difficulty putting food on the table for her family during the holidays.

In addition to money directly stolen, affected customers faced higher interest rates due to missed payments, costs of replacing government-issued identification, and the hiring of legal help. One customer had 35 fraudulent inquiries on his credit records, and his "credit score dropped approximately 25 to 50 points," delaying the purchase of a desperately needed newer car.[114]

[h] Track data is a string of characters encoded on the magnetic strip of a credit card that includes the cardholder's name, card expiration date, and the Card Verification Value (CVV) number.

Plaintiffs in lawsuits filed by consumers claimed that Target had a responsibility to adhere to industry standards in building and maintaining firewalls, protecting cardholder data, and monitoring controls and network systems. The consumer suits alleged that Target was not compliant with all of the regulations applicable to retailers. In addition, Target's delays in discovering the breach, from November 30–December 12, and stopping the breach, from December 12–December 15, allowed hackers to continue stealing credit and debit card information.

As a result, affected customers sought restitution for violations of state consumer laws, negligence, and breach of contract. In November 2015, Target agreed to a settlement to cover consumer losses.[115] Sixty-one million people were directly notified of the settlement deal, and customers who documented their expenses could recover up to $10,000.[i,116]

Banks

Visa, MasterCard, and other financial institutions also filed lawsuits against Target. At least seven months before the attacks, in April and again in August 2013, Visa had published alerts to retailers detailing security vulnerabilities to the RAM scraper malware.[117,118] Visa detailed the methods hackers could use and recommended steps such as "firewall configuration," "ensure[ing] only allowed ports, services and IP addresses are communicating with the network," "segregate payment processing network from other non-payment processing networks," and "implement hardware-based point-to-point encryption."[119] Target's in-house security team escalated the alerts and asked for a further review of Target's security infrastructure, but the request was not acted upon.[120]

Banks claimed that Target was negligent in not providing sufficient data security. Plaintiffs also charged Target with violating the Minnesota Plastic Card Security Act by inadequately securing the data, misrepresenting facts about its data security, and retaining payment card data.[121]

In addition, because Target processed credit cards, it was subject to the FACTA Red Flag Rules.[j,122] These rules required retailers to develop and administer protocols to identify data theft and vulnerabilities, monitor credit transactions, and respond when consumer identities were stolen. Banks argued that Target failed to implement or adhere to the "Red Flag Rules," violating federal law.[123]

"Financial institutions should not have to bear the burden of extensive costs related to merchant data breaches over which they have no control," argued the plaintiff attorneys.[124] One affected bank claimed that Target's systems were vulnerable, as Target retained customer transaction data on its own servers. As a result, banks faced additional costs from reissuing cards, reimbursing customers who incurred unauthorized charges, and adding staff to provide customer care.[125] These costs were expensive for smaller banks in particular, as explained by the CEO of the American Bankers Association. In a letter to Congress on January 16, 2014, he explained:[126,127]

> Those [banks] with under $1 billion in assets spent an average of $11.02 to reissue a debit card and $12.75 to reissue a credit card. That compares with $2.70 and $2.99 respectively for banks with more than $50 billion in assets. . . . When a retailer like Target

[i] Those customers who did not document their losses were entitled to an equal portion of the remaining settlement fund.

[j] Section 114 of The Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), known as the "Red Flag Rules," requires organizations that arrange for or extend credit to detect, prevent, and mitigate identity theft by developing a written "Identity Theft Prevention Program." This definition covers not only financial institutions but also nonfinancial companies such as utilities, car dealers, health-care companies, and retailers.

> speaks of its customers having "zero liability" from fraudulent transactions, it is because our nation's banks are providing that relief, not the retailer that suffered the breach.

Target settled its complaint from Visa for $67 million in August 2015, and for roughly $40 million with MasterCard and other banks in December 2015.[128,129] By then, Target had spent roughly $290 million in costs related to the breach and expected a reimbursement of $90 million from insurers.[130]

Board Accountability

Shareholders of Target filed derivative lawsuits against all directors on the firm's board of directors and against the CFO and CIO.[131] In particular, shareholders identified CEO Gregg W. Steinhafel, CIO Beth M. Jacob, Lead Independent Director James A. Johnson, and chairs and members of the board's Audit and Corporate Responsibility committees as leaders whose "reckless disregard for their duties . . . posed a risk of serious injury to the Company."[132] (Refer to **Exhibit 9** for biographic information on Target's directors.)

The lawsuits claimed that by virtue of their fiduciary duties, the directors were required to create and maintain a system to protect customers' personal and financial information, as well as to inquire into and correct unsound practices. In addition, the directors were required to inform customers of a breach accurately and in a timely manner.[133]

The derivative lawsuits stated that the directors breached their fiduciary duty by failing to implement internal controls to protect consumer data.[134] In addition, shareholders alleged the directors' negligence caused a waste of corporate assets, as the firm lost revenue, had to offer a 10% discount to draw customers back to the store, and faced upcoming litigation expenses.[135] Plaintiffs also charged that the directors wasted and mismanaged corporate assets by providing improper compensation and bonus structures to certain executive officers.[136]

Plaintiffs further alleged that the directors and Audit Committee members did not take their financial reporting responsibilities seriously and that they failed to supervise internal controls and cyber security systems.[137] Shareholders listed a number of costs incurred by them from the directors' inactions—class-action settlements, DOJ and Secret Service investigations and possible fines, increased cost of capital due to a ratings downgrade, legal and consulting fees, and costs of the customer-retention efforts such as credit monitoring and 10% discount to U.S. shoppers—all of which eroded shareholder value.[138]

In response, Target's lawyers claimed that directors were not liable, as they were shielded by the firm's Articles of Incorporation, which protected directors from liability except in cases of intentional misconduct. In addition, the legal team responded that shareholders had failed to provide "plausible claims" that the directors failed to discharge their duties and that occurrence of the data breach in and of itself did not imply that the directors failed in their duties.[139]

Risks Acknowledged by Target

The Target board's Audit Committee charter highlighted the committee's oversight responsibility for reviewing and discussing the approach to risk assessment, including the risk of fraud, with the firm's head of internal audit.[140] This collaborative responsibility also included dedicating resources to mitigate identified risks.[141,142] Target's proxy statement also highlighted the Corporate Responsibility Committee's responsibility for "assessing and managing reputational risk."[143,144] In fact, in its 2012 10-K filing, Target had identified data security breach as a risk the firm was exposed to:

> If we experience a significant data security breach or fail to detect and appropriately respond to a significant data security breach, we could be exposed to government enforcement actions and private litigation. In addition, our guests could lose confidence in our ability to protect their personal information, which could cause them to discontinue usage of REDcards, decline to use our pharmacy services, or stop shopping with us altogether. The loss of confidence from a significant data security breach involving team members could hurt our reputation, cause team member recruiting and retention challenges, increase our labor costs and affect how we operate our business.[145]

Governance Institutions Weigh In

Leading proxy advisory firm ISS issued a report in May 2014, stating that failures of the Audit Committee, the Corporate Responsibility Committee, and the board allowed significant losses to the company and its shareholders. ISS expressed concern at the "failure of these committees and possibly by extension the full board, to recognize the potential threat faced by the company."[146] ISS advised shareholders that 7 of 10 board members should be removed for their negligence. ISS recommended removal of the entire Audit Committee, including the chair, Roxanne Austin; the Lead Independent Director, James Johnson, who was also on the Compensation Committee; and two other directors.[147]

ISS reasoned that by failing to closely monitor the possibility of theft, the directors allowed their customers and communities to face undue risks and insurmountable damage to the firm's brand and reputation. The ISS report stated:[148]

> It appears that failure of the [Audit and Corporate Responsibility] committees to ensure appropriate management of these risks set the stage for the data breach, which has resulted in significant losses to the company and its shareholders. . . . A vote AGAINST directors serving on the Audit and Corporate Responsibility Committees is warranted for failure to provide sufficient risk oversight.

ISS also stated that the board displayed a disregard for disclosure procedures and risk assessment processes by not conveying a robust program to shareholders before the breach.[149] The board's response to the breach had been reactionary, suggesting that the firm was unprepared to prevent and handle a breach of this magnitude.[150] ISS also stated that both the Audit and Corporate Responsibility committees should have more closely monitored the risk to brand value and firm reputation, and hence these committees were responsible for losses due to the data breach.[151]

ISS questioned whether the CIO was qualified for the role. The report stated:

> According to a publicly available biography, the former CIO first joined Target in 1984, spending two years as an assistant buyer in the company's Dayton's department store division. She left the company in 1986, but returned in 2002 as director of guest contact centers. She became vice president of guest operations in 2006, then was named senior vice president and CIO in 2008. She was promoted to executive vice president and CIO in 2010. In comparison, the new CIO has "more than 40 years of experience and is a recognized leader in information technology, data security, and business operations," according to Target's press release announcing his appointment.[152]

However, Glass Lewis, another proxy advisor, suggested that there wasn't enough information to conclude that the board had been negligent.[153] Glass Lewis acknowledged several failings—Target had failed to require appropriate authentication from its vendors, its employees failed to act on security warnings, and the system allowed transmission of stolen data without detection and failed to detect

that internal servers had been compromised. However, Glass Lewis did not recommend replacing any directors due to the data breach.[154] Instead, Glass Lewis recommended "no" votes against Johnson and Anne M. Mulcahy for unrelated issues at Fannie Mae and Citigroup, respectively.

Target's Board Defends Itself

After ISS released its report, Target's board issued a letter assuring shareholders that it took its "oversight responsibilities seriously" and before the breach had authorized the company to spend "hundreds of millions of dollars" on network security, doubled the information security staff over five years, and taken other security measures.[155] (See **Exhibit 10** for the letter.) Target also explained that the firm had "300 employees dedicated to information security, trained 350,000 employees on data security, and staffed a 24-hour security operations center to review suspicious network activity."[156] Others defended the board as well. A governance expert explained, "The role of directors is one of oversight, not of day to day management. Directors cannot be expected to manage security personnel to ensure that they are doing their job; this role is clearly and squarely a management function. . . . Target did identify cyber security as a risk, and placed controls to monitor this risk; the oversight was the result of human error."[157]

According to some industry analysts, cyber breaches into corporate networks were risks that could be managed but not prevented. (Refer to **Exhibits 11** and **12a, 12b,** and **12c** for statistics on cyber breaches in the U.S.) According to these analysts, it was important for management to respond quickly once the breach was discovered, and in their judgment, Target's management was quick to respond in this case. As such, these analysts believed the argument to blame board members was not particularly strong compared to prior breaches that went undetected for years.[158]

Conclusion

Data breaches and cyber crime had become an increasing problem for U.S. corporations in recent years. Faced with these trends, observers and governance experts wondered what role the board of directors should play in overseeing cyber security and how boards could most effectively carry out their responsibilities in this domain.

Exhibit 1 Target Corporation's Selected Income Statement (millions, $USD)

Fiscal Year Ending February-01	2010	2011	2012	2013	2014
Revenue	63,435	65,786	68,466	71,960	71,279
Gross Profit	19,031	20,703	21,559	22,427	21,240
Net Income	2,488	2,920	2,929	2,999	1,971
Basic EPS	3.31	4.04	4.31	4.57	3.1
Weighted Avg. Basic Shares Out.	752	724	679	657	635

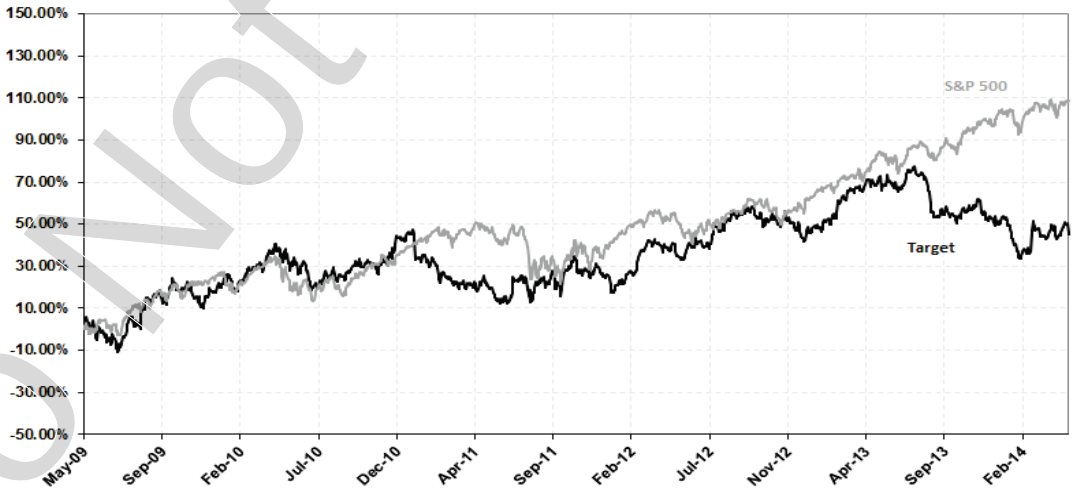
Source: Capital IQ, accessed June 8, 2016.

Exhibit 2 Target Corporation's Selected Balance Sheet (millions, $USD)

Fiscal Year Ending February-01	2010	2011	2012	2013	2014
Total Current Assets	18,424	17,213	16,449	16,388	11,573
Goodwill	59	59	59	59	151
Total Assets	44,533	43,705	46,630	48,163	44,553
Total Current Liabilities	11,327	10,070	14,287	14,031	12,777
Total Liabilities	29,186	28,218	30,809	31,605	28,322
Total Equity	15,347	15,487	15,821	16,558	16,231
Total Liabilities And Equity	44,533	43,705	46,630	48,163	44,553

Source: Capital IQ, accessed June 8, 2016.

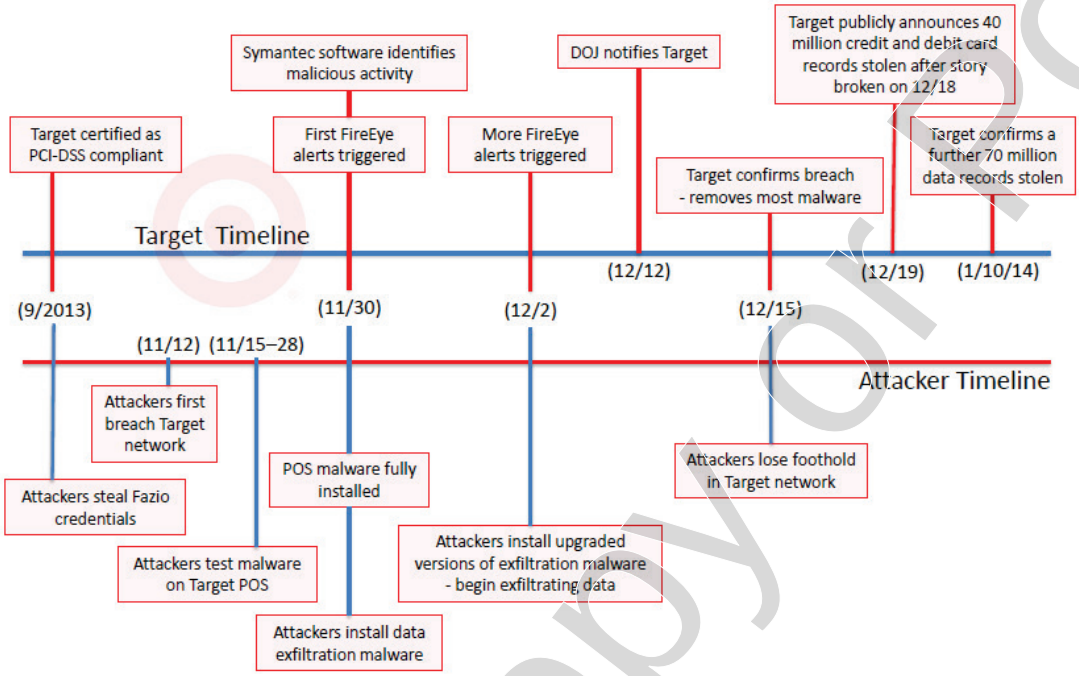
Exhibit 3 Target Corporation's Stock Performance vs. S&P 500 (May 5, 2009–May 5, 2014)



Source: Capital IQ, accessed May 2, 2016.

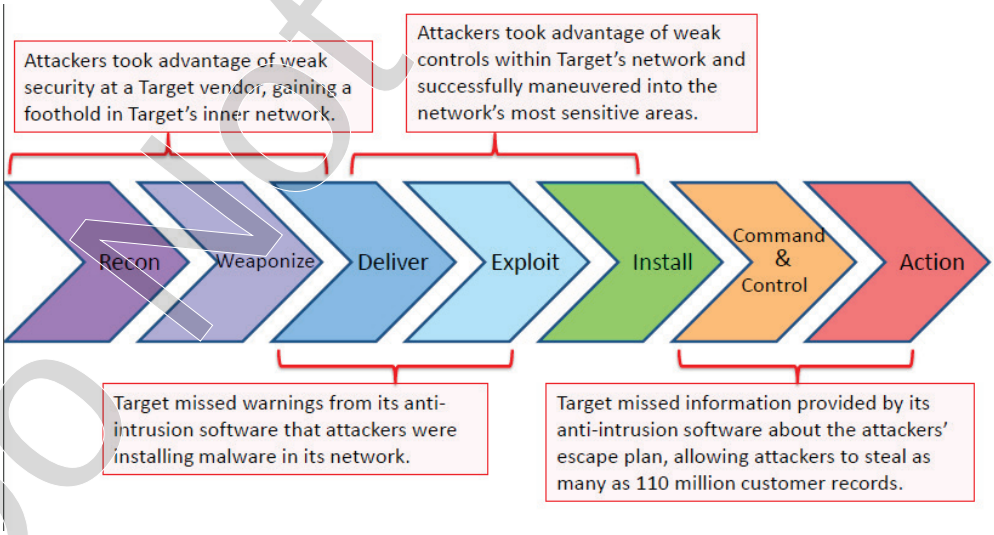
Note: Both series are indexed to May 5, 2009.

Exhibit 4 A Timeline of the Target Data Breach



Source: Senate Committee on Commerce, Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach*, 113th Cong., 2nd sess., 2014.

Exhibit 5 Target's Possible Missed Opportunities



Source: Senate Committee on Commerce, Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach*, 113th Cong., 2nd sess., 2014.

Exhibit 6 Summary of Senate Committee Analysis of the Target Data Breach

The following summary describes the "Kill Chain" analysis undertaken by the Senate Committee and describes the steps that Target and Fazio Mechanical Services could have taken to prevent the cyberattack.

1) **"Reconnaissance"**—Information about victims gathered quietly by attacker
   Attackers may have sent emails with malware to Fazio, Target's external vendor. Simple internet searches enabled hackers to find Target's supplier portal and facilities management pages, and map out Target's internal network. Target could have limited publicly available information.

2) **"Weaponization"**—Hacker prepares the malware to be sent to victim
   Through a simple email attachment such as a PDF or Microsoft Office document, the hacker likely weaponized its malware. Fazio improperly used a free version of its anti-malware software, which did not provide real-time protection, and was intended for individual and not corporate use.

3) **"Delivery"**—Malware sent to victim
   The attacker began the phishing attack, and the malware provided hackers with Fazio's passwords to Target's systems (Target could have required two-step authentication at this stage, a password and a mobile confirmation, as a protective measure). PCI-DSS standards require two-step authentication for remote access to payment networks, but this was not technically a part of Target's POS system. Attackers uploaded the RAM scraping malware to Target's POS terminals.

4) **"Exploitation"**—Malware deployed in victim's networks
   The RAM scraping malware started recording data of millions of cards as they were swiped at registers. At this step, Target could have checked any of the alerts sent by its FireEye software, or it could have enabled the software to automatically delete the malware. Target could also have paid greater attention to one of many industry and government alerts of increased cyber threats.

5) **"Installation"**—Attacker gains ground in victim's networks
   Hackers used Fazio's systems to further breach Target's networks, although it is unclear how. A protective step at this stage would have been to delete unneeded default accounts.

6) "**Command and Control (C2)"**—Attacker gains remote access to victim's networks
   Hackers maintained a line of communication between the outside internet and Target's network—Target could have checked why Fazio's logon was being used to access unrelated parts of Target's network, and could have developed stronger firewalls.

7) **"Actions on Objectives"**—Attacker initiates data extraction
   Hackers extracted the data to servers in Russia, which should have been flagged as suspicious. Target's FireEye system did detect the extraction malware, and Target could have acted on this.

Source: Senate Committee on Commerce, Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach,* 113th Cong., 2nd sess., 2014.

Note: A "Kill Chain" analysis is a framework developed by Lockheed Martin security researchers, and is an industry standard tool used by the information security industry.

Exhibit 7 Target's Pre-Breach Information Security Structure

Three teams at Target had interrelated responsibility for data security. These were the Target Information Protection (TIP); Target Technology Services (TTS); and Corporate Security.

Target Information Protection (TIP)

TIP's role included: (1) establish and implement information security policies and standards; (2) work with third-party assessors to manage compliance with external standards; (3) manage response to non-routine network security incidents; (4) prioritize information-security related investments.

From 2010 until the breach, TIP was led by a senior director–level executive who, along with responsibility for aspects of data security, was also the Chief Privacy Officer and was responsible for HIPAA compliance. The TIP senior director reported to the President of Target Financial and Retail Services (FRS) division, who in turn reported to the CFO of the company. TIP had teams related to aspects of security, in particular:

(a) Vendor Assessment and Management Team, which was responsible for assessing whether vendors would be able to access Target's network based on vendor risk. The team conducted around 300 vendor assessments each year.

(b) Risk Review Committee (RRC), which was a cross-functional team that served as resource that provided guidance to business and technology teams on risk mitigation. RRC did not manage the mitigation but served as a source of information.

(c) Intake team, which provided a venue for Target employees to direct security-related questions, e.g., what to do if an employee lost a laptop?

Target Technology Services (TTS)

TTS was the information technology team led by the Chief Information Officer (CIO), who in turn reported to the CEO of the company. TTS planned, built, and ran Target's computer systems and managed the corporate network, data centers, store networks, point-of-sale registers, and the website Target.com. TTS employed around 9,000 people at the time of the breach. TTS had a cybersecurity team led by a senior director who reported to the CIO. In addition, Target had two other teams relating to information security within TTS: the Security Operations Center (SOC) and the Red team.

(a) The SOC was a 24-hour alert management center that monitored the network for anomalous activity and worked with TIP to address identified security issues. At the time of the breach, Target's systems generated about 200 alerts per day, which were all analyzed by humans within a predefined system of analysis and escalation. If an alert was deemed serious, it was escalated to TIP for resolution.

(b) The Red team was an internal team of "white hat" hackers that conducted network security tests and simulated covert and overt attacks to test Target's responses.

Corporate Security and Information Security Investigations (ISI)

The investigative arm of the data security program and the cyber intelligence team was part of the Corporate Security department, headed by a Vice President, who reported to the General Counsel. ISI analysts investigated incidents in coordination with the SOC and TIP.

Cybersecurity Program Governance

Overall governance of cyber security was under the purview of Target's Cyber Executive Committee that met quarterly. The committee consisted of senior managers from Corporate Security, FRS business unit, and TTS. The next level was the Cyber Steering Committee, which was charged with bringing people together to plan the future of the cyber security program, review cyber security strategy, and prepare agendas for the Cyber Executive Committee meetings. It consisted of leaders from TTP, TTS, and Corporate Security. Finally, the Cyber Working Group gathered relevant information from internal and external sources and reported to the Cyber Steering Committee on threat and vulnerability trends. The members of this group came from TIP, TTS, and Corporate Security.

Internal and External Auditors

The Assurance, Risk, and Compliance (ARC) department performed the company's internal audit function and reported to the CFO and the Audit Committee. The internal audit function included a team that was responsible for auditing the effectiveness of controls for support functions, including information technology. Ernst & Young (E&Y), the external auditors of Target, tested and audited internal controls related to information technology. Prior to the breach, E&Y had found no material weaknesses in Target's internal controls.

Board Committees

Prior to the breach, the oversight responsibility relating to data security belonged mainly to the Audit Committee as part of its overall responsibility for monitoring the integrity of Target's financial statements, monitoring internal audit, and monitoring Target's compliance with legal and regulatory requirements. The Corporate Responsibility Committee had oversight duties pertaining to customer privacy and the impact of a breach on Target's reputation.

Source: Compiled by casewriter based on the information in the Report of the Special Litigation Committee of Target Corporation dated March 30, 2016.

Exhibit 8a Target's Initial Press Release, Dated December 19, 2013

Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores

Target today confirmed it is aware of unauthorized access to payment card data that may have impacted certain guests making credit and debit card purchases in its U.S. stores. Target is working closely with law enforcement and financial institutions, and has identified and resolved the issue.

"Target's first priority is preserving the trust of our guests and we have moved swiftly to address this issue, so guests can shop with confidence. We regret any inconvenience this may cause," said Gregg Steinhafel, chairman, president and chief executive officer, Target. "We take this matter very seriously and are working with law enforcement to bring those responsible to justice."

Approximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013. Target alerted authorities and financial institutions immediately after it was made aware of the unauthorized access, and is putting all appropriate resources behind these efforts. Among other actions, Target is partnering with a leading third-party forensics firm to conduct a thorough investigation of the incident.

More information is available at Target's corporate website. Guests who suspect unauthorized activity should contact Target at: 866-852-8680.

Source: "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores," Target Corporation website, https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car accessed July 7, 2016.

Exhibit 8b Target's CEO Informs Customers of Data Breach, Dated December 20, 2013

Dear Target Guest,

As you have likely heard by now, Target experienced unauthorized access to payment card data from U.S. Target stores. We take this crime seriously. It was a crime against Target, our team members and most importantly you—our valued guest.

We understand that a situation like this creates stress and anxiety about the safety of your payment card data at Target. Our brand has been built on a 50-year foundation of trust with our guests, and we want to assure you that the cause of this issue has been addressed and you can shop with confidence at Target.

We want you to know a few important things:

The unauthorized access took place in U.S. Target stores between Nov. 27 and Dec. 15, 2013. Canadian stores and target.com were not affected.

Even if you shopped at Target during this time frame, it doesn't mean you are a victim of fraud. In fact, in other similar situations, there are typically low levels of actual fraud.

There is no indication that PIN numbers have been compromised on affected bank issued PIN debit cards or Target debit cards. Someone cannot visit an ATM with a fraudulent debit card and withdraw cash.

You will not be responsible for fraudulent charges—either your bank or Target have that responsibility.

We're working as fast as we can to get you the information you need. Our guests are always the first priority.

For extra assurance, we will offer free credit monitoring services for everyone impacted. We'll be in touch with you soon on how and where to access the service.

Please read the full notice below. And over the coming days and weeks we will be relying on target.com, abullseyeview.com, corporate.target.com and our various social channels to answer questions and keep you up to date.

Thank you for your patience, understanding and loyalty to Target!

Gregg Steinhafel Chairman, President and CEO, Target

Source: Target Corporation, "A message from CEO Gregg Steinhafel about Target's payment card issues," Target Corporation website, https://corporate.target.com/article/2013/12/important-notice-unauthorized-access-to-payment-ca, accessed May 4, 2016.

Exhibit 9 Target Corporation's 2013 Board of Directors

Roxanne S. Austin, 52. President of Austin Investment Advisors. Director since 2002.
Committees: Audit (Chair), Finance.

Ms. Austin provides the Board with financial, operational and risk management expertise, and substantial knowledge of new media technologies, which were developed during Ms. Austin's previous service as President and COO of DirecTV, Executive Vice President and CFO of Hughes Electronics Corporation and Partner of Deloitte & Touche.

Douglas M. Baker, Jr., 53. Chairman and Chief Executive Officer of Ecolab Inc. Director since 2013.
Committees: Audit, Nominating & Governance.

Mr. Baker provides the Board with valuable global marketing, sales and general management experience, as well as operational and governance perspectives. His current role as CEO of a large publicly-held company provides the Board with additional top-level perspective in organizational management.

Henrique De Castro, 47. Chief Operating Officer of Yahoo! Inc. Director since 2013.
Committees: Corporate Responsibility, Nominating & Governance.

Mr. De Castro provides the Board with valuable insight into media, mobile and technology platforms. His experiences at Yahoo! and Google, as well as his prior experience at Dell Inc. provides him with global perspectives on leading operations, strategy, partner management and revenue generation in the technology and media industries.

Calvin Darden, 63. Chairman of Darden Development Group, LLC. Director since 2003.
Committees: Compensation, Nominating & Governance.

Mr. Darden provides the Board with significant experience in supply chain networks, logistics, customer service and management of a large-scale workforce obtained over his 33-year career with United Parcel Service of America, Inc., and more recently has developed expertise in community relations and real estate development.

James A. Johnson, 69. Founder of Johnson Capital Partners. Director since 1996.
Committees: Compensation (Chair), Corporate Responsibility.

Mr. Johnson has more than 40 years of experience in the business and public sectors. Mr. Johnson provides the Board with strong leadership and consensus-building capabilities as well as a solid understanding of public policy dynamics, corporate governance and reputation management issues.

Mary E. Minnick, 53. Partner of Lion Capital. Director since 2005.
Committees: Audit, Corporate Responsibility.

Ms. Minnick provides the Board with substantial expertise in building brand awareness, general management, product development, marketing, distribution and sales on a global scale obtained over her 23-year career with The Coca-Cola Company. Her current position with Lion Capital provides the Board with additional insights into the retail business and consumer marketing trends outside the United States.

Anne M. Mulcahy, 60. Chairman of the Board of Trustees of Save The Children Federation, Inc. Director since 1997.
Committees: Nominating & Governance (Chair), Finance.

Ms. Mulcahy obtained extensive experience in all areas of business management as she led Xerox through a transformational turnaround. This experience, combined with her leadership roles in business trade associations and public policy activities, provides the Board with additional expertise in the areas of organizational effectiveness, financial management and corporate governance.

Derica W. Rice, 48. Executive Vice President, Global Services and Chief Financial Officer of Eli Lilly and Company. Director since 2008.
Committees: Finance (Chair), Audit.

Mr. Rice's career with Eli Lilly has provided him with substantial experience in managing worldwide financial operations. His expertise gives the Board additional skills in the areas of financial oversight, risk management and the alignment of financial and strategic initiatives.

Gregg W. Steinhafel, 58. Chairman of the Board, Chief Executive Officer and President of Target. Director since 2007.
Committees: None

In his more than 30 years at Target, Mr. Steinhafel has gained meaningful leadership experience and retail knowledge. As Chief Executive Officer, he is responsible for determining Target's strategy and clearly articulating priorities, as well as aligning and motivating the organization to execute effectively and ensure continued success. These capabilities, combined with Mr. Steinhafel's intimate understanding of Target's guests and unwavering commitment to Target's brand, make him uniquely qualified to serve on the Board.

John G. Stumpf, 59. Chairman of the Board, President and Chief Executive Officer of Wells Fargo & Company. Director since 2010.
Committees: Compensation, Finance.

Mr. Stumpf's current role as Chairman, President and Chief Executive Officer of Wells Fargo, and long career in banking, provides the Board with expertise in brand management, financial oversight and stewardship of capital.

Solomon D. Trujillo, 61. Chief Executive Officer and a director of Telstra Corporation Limited. Director since 1994.
Committees: Corporate Responsibility (Chair), Nominating & Governance.

Mr. Trujillo is an international business executive with three decades experience as CEO of large market cap global companies in the telecommunications, media and cable industries headquartered in the United States, the European Union and the Asia-Pacific region. He has global operations experience and provides the Board with substantial international experience and expertise in the retail, technology, media and communications industries.

Source: Target 2013 Proxy Statement, accessed May 4, 2016.

Exhibit 10 Target's Interim Chairwoman Roxanne Austin Defends the Board of Directors

To Our Shareholders,

As you make your voting decisions for our 2014 Annual Meeting, we wanted you to have the facts about your Board's oversight of information security practices at Target.

Cyber-crime is a real and persistent threat as sophisticated criminals are constantly seeking to breach information networks and steal data. Breaches are occurring across the economy and are affecting a wide range of victims including the US Government, the technology and defense industries, and more traditional companies, like retailers.

Your Board fully recognizes the importance of its oversight responsibilities in this area. Under the Board's leadership and oversight, Target took significant action to address evolving cyber-crime risks before the breach, by:

- Investing hundreds of millions of dollars in network security personnel, processes, technology and related resources
- Dedicating more than 300 employees to information security (more than double from five years ago)
- Requiring annual data security training for all Target employees (more than 350,000)
- Operating a Security Operations Center (SOC) staffed around the clock with trained professionals to review suspicious network activity
- Investing in network monitoring technology to enhance Target's ability to detect potential cyber-attacks
- Becoming a founding member of the National Cyber-Forensics & Training Alliance (NCFTA), a partnership of public, private and academic participants focused on identifying, mitigating and neutralizing cyber-threats

Despite these efforts, Target suffered a sophisticated criminal attack that led to our data breach in 2013. Since then, your Board has actively monitored Target's response to the situation. Following the breach, the Board has overseen substantial efforts to protect Target's guests. Target is undertaking an end-to-end review of its network security and is moving toward chip and PIN technology for credit card processing. The Board is conducting a broad examination of Target's risk oversight structure, which will include an examination of the role of senior management, reporting structures and Board oversight.

Target has already done the following:

- Announced that we are accelerating the adoption of "chip and PIN" smart payment card technology and set important goals for 2015, including:
  - Converting all of our REDcards to chip-enabled cards
  - Equipping our stores with chip-enabled card readers
- Hired a new Chief Information Officer
- Elevated the Chief Information Security Officer and Chief Compliance Officer roles and commenced searches to fill those positions

- Enhanced information security decision making processes
- Worked with other leading retailers to establish the Retail Information Sharing and Analysis Center (Retail-ISAC) and joined the Financial Services Information Sharing and Analysis Center (FSISAC) as the first retail member of the group

Again, we want to assure you that the Board takes its oversight responsibilities seriously and we recognize the importance of Target addressing these information security issues in the most effective manner possible. We would appreciate your feedback on this important topic. If you would like to share your thoughts and comments, please send a message to BoardOfDirectors@target.com. We also value your support and ask that you vote in favor of the re-election of all your Target directors at our 2014 Annual Meeting.

Roxanne Austin, Interim Chair of the Board of Directors

Source: Target Def 14A filed June 2, 2014, accessed May 12, 2016.

Exhibit 11 Large Retail Cyberattacks

According to industry reports, cyberattacks in the retail industry have increased dramatically since 2009, with over 100 breaches in retail being reported in 2012:

During this time period, hackers targeted fewer, but larger retailers with access to large portions of the U.S. population—TJX Companies (2007, 100 million), The Home Depot (2014, 56 million), The Valve Corporation (2011, 35 million) and Sony PlayStation Network (2011, 12 million).

Industry experts found that over 99% of the attacks directly exploited a target endpoint, or successfully deployed malware. One reason why these strategies had been successful was because of a lack of data validation by security administrators, and due to the innate complexity of protecting against a large volume of attacks. As a result, hacking and malware became the most popular method of attack, and from 2005–2014, over 300 million records were lost solely by these methods.

Source: David McMillen, IBM Research and Intelligence Report, IBM Corporation, January 6, 2015.

Exhibit 12a Industries Targeted by Cyber Breaches, 2011–2013

Industry Sector	# of Breaches 2011	% of Total Breaches 2011	# of Breaches 2012	% of Total Breaches 2012	# of Breaches 2013	% of Total Breaches 2013
Business	177	42%	162	34%	195	32%
Educational	57	14%	63	13%	54	9%
Government/Military	54	13%	55	12%	60	10%
Health/Medical	102	24%	167	36%	271	44%
Financial/Credit	31	7%	24	5%	34	6%
Total	**421**		**471**		**614**	

Exhibit 12b Techniques Used by Cyber Criminals, 2011–2013

Type of Incident	# of Breaches 2011	% of Total Breaches 2011	# of Breaches 2012	% of Total Breaches 2012	# of Breaches 2013	% of Total Breaches 2013
Insider Theft	56	13%	40	9%	72	12%
Hacking	110	26%	128	27%	160	26%
Data on the Move	78	19%	57	12%	79	13%
Accidental Exposure	45	11%	41	9%	46	8%
Subcontractor	32	8%	54	12%	89	15%
Employee Negligence			34	7%	58	10%

Exhibit 12c Consumer Data Lost, 2011–2013

Category	# of Breaches 2011	% of Total Breaches 2011	# of Breaches 2012	% of Total Breaches 2012	# of Breaches 2013	% of Total Breaches 2013
Paper	68	16%	72	15%	73	12%
Unknown Totals	172	41%	237	50%	243	40%
Exposed Social Security Numbers	260	62%	226	48%	295	48%
Exposed Credit/Debit Cards	111	26%	68	14%	96	16%
Unknown Attributes	133	32%	163	35%	176	29%

Source: Identity Theft Resource Center, http://www.idtheftcenter.org/images/breach/2005to2015multiyear.pdf, accessed May 4, 2016.

Exhibit 13 Target's Board of Director Election Results, 2014 (thousands)

	For		Against	
Nominee	**Shares**	**%**	**Shares**	**%**
Roxanne S. Austin	382,077	78.0	107,814	22.0
Douglas M. Baker, Jr.	467,403	95.5	22,107	4.5
Calvin Darden	389,118	79.5	100,313	20.5
Henrique De Castro	396,684	81.0	93,130	19.0
James A. Johnson	307,783	62.9	181,383	37.1
Mary E. Minnick	391,561	80.0	97,848	20.0
Anne M. Mulcahy	310,851	63.6	177,938	36.4
Derica W. Rice	393,117	80.3	96,243	19.7
Kenneth L. Salazar	475,251	97.1	14,167	2.9
John G. Stumpf	464,751	94.9	24,829	5.1

Source: Target, 2014 Form 8-K, accessed May 4, 2016.

Endnotes

[1] Target Corp., 2013 10-K.

[2] Target Corporation, "Target through the years," Target Corporation website, https://corporate.target.com/about/history/Target-through-the-years, accessed May 1, 2016.

[3] K. Palepu, S. Srinivasan, and J. Weber, "Target Corporation: Ackman versus the Board," HBS No. 109-010 (Boston: Harvard Business School Publishing, 2011).

[4] "Target Corp. Stock Report," S&P Capital IQ, March 25, 2014.

[5] Ibid.

[6] Ibid. (CAGR are authors' calculations).

[7] Target Corp., 2013 10-K.

[8] Target Corporation, "Target Reports Third Quarter 2013 Earnings," Target Corporation website, http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1878983, accessed May 26, 2016.

[9] Target Corporation, "Target Corporation Increases Regular Quarterly Dividend by 19 Percent," Target Corporation website, http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1829310, accessed May 26, 2016.

[10] Brad Dorfman, "Target CEO sees shoppers re-emerging," Reuters, May 7, 2010.

[11] Target Corp., 2013 10-Q.

[12] Target Corp., 2013 10-K.

[13] Target Corp., 2010 10-K; Target Corp., 2011 10-K; Target Corp., 2012 10-K; Target Corp., 2013 10-K; and author's calculations.

[14] In re: Target Corp. Customer Data Security Breach Litigation, No 0:14-md-02522, Complaint (D. Minn. filed Aug. 25, 2014).

[15] SearchSecurity, "phishing," SearchSecurity website, http://searchsecurity.techtarget.com/definition/phishing, accessed May 2, 2016.

[16] In re: Target Corp. Customer Data Security Breach Litigation, No 0:14-md-02522, Complaint (D. Minn. filed Aug. 25, 2014).

[17] Ibid.

[18] Ibid.

[19] Brian Krebs, "Email Attack on Vendor Set Up Breach at Target," *Krebs on Security* (blog), February 14, 2014.

[20] In re: Target Corp. Customer Data Security Breach Litigation, No 0:14-md-02522, Complaint (D. Minn. filed Aug. 25, 2014).

[21] Brian Krebs, "Email Attack on Vendor Set Up Breach at Target."

[22] In re: Target Corp. Customer Data Security Breach Litigation, No 0:14-md-02522, Complaint (D. Minn. filed Aug. 25, 2014).

[23] Ibid.

[24] Ibid.

[25] SearchSecurity, "malware (malicious software)," SearchSecurity website, http://searchmidmarketsecurity.techtarget.com/definition/malware, accessed May 2, 2016.

[26] Matthew J. Schwartz, "Target Breach: 8 Facts On Memory-Scraping Malware," *Dark Reading*, January 14, 2014.

[27] Senate Committee on Commerce, Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach,* 113th Cong., 2nd sess., 2014.

[28] N. Perlroth, "Credit Card Data Theft at Target Investigated," *New York Times*, December 19, 2013.

[29] Senate Committee on Commerce, Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach,* 113th Cong., 2nd sess., 2014.

[30] Ibid.

[31] Ibid.

[32] Target Corp., 2013 10-K.

[33] Elizabeth A. Harris and Nicole Perlroth, "For Target, the Breach Numbers Grow," *New York Times,* January 10, 2014.

[34] In re: Target Corp. Customer Data Security Breach Litigation, No 0:14-md-02522, Complaint (D. Minn. filed Aug. 25, 2014).

[35] Ibid.

[36] Ibid.

[37] Mellisa Tolentino, "Which stores open early on Thanksgiving Day? Beat Black Friday," *Silicon Angle*, November 26, 2014.

[38] Emily J. Fox, "Wal-Mart workers plan Black Friday walkout," CNN Money, November 15, 2012.

[39] Senate Committee on Commerce, Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach,* 113th Cong., 2nd sess., 2014.

[40] Kevin Fogarty, "Report: Target Bosses Ignored IT Alert of Impending Breach," *Dice*, March 13, 2014.

[41] Robert Lemos, "Target Breach Involved Two-Stage Cyber-Attack: Security Researchers," *eWeek*, January 21, 2014.

[42] Kevin Fogarty, "Report: Target Bosses Ignored IT Alert of Impending Breach."

[43] Mary Shacklett, "A former CIO's take on Target CIO resigning after massive data breach," *TechRepublic*, March 13, 2014.

[44] Ibid.

[45] Target Corporation, "Testimony of John Mulligan," Target Corporation website, https://corporate.target.com/_media/TargetCorp/global/PDF/Target-SJC-020414.pdf, accessed May 26, 2016.

[46] In re: Target Corp. Customer Data Security Breach Litigation, No 0:14-md-02522, Complaint (D. Minn. filed Aug. 25, 2014).

[47] Meagan Clark, "Timeline of Target's Data Breach And Aftermath: How Cybertheft Snowballed For The Giant Retailer," *International Business Times*, May 5, 2014.

[48] In re: Target Corp. Customer Data Security Breach Litigation, No 0:14-md-02522, Complaint (D. Minn. filed Aug. 25, 2014).

[49] Ibid.

[50] Becky Quick and Matthew J. Belvedere, "Target CEO 'still shaken' by the data breach, vows to 'make it right,'" CNBC, January 12, 2014.

[51] Natalie Burg, "Five Lessons For Every Business From Target's Data Breach," *Forbes Business*, January 17, 2014.

[52] Senate Committee on Commerce, Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach,* 113th Cong., 2nd sess., 2014.

[53] Brian Krebs, "Sources: Target Investigating Data Breach," *Krebs on Security* (blog), December 18, 2013.

[54] Ibid.

[55] In re: Target Corp. Customer Data Security Breach Litigation, No 0:14-md-02522, Complaint (D. Minn. filed Aug. 25, 2014).

[56] Congressional Research Services, The Target and Other Financial Data Breaches: Frequently Asked Questions, 114th Cong., 1st sess. 2015.

[57] Target Corporation, "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores," Target Corporation website, https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car, accessed May 4, 2016.

[58] Tim Feran, "Delaware woman among Target data-breach victims," *Columbus Dispatch*, December 20, 2013.

[59] Beth Pinsker, "Consumers vent frustration and anger at Target data breach," Reuters, January 13, 2014.

[60] Target Corporation, "Target invests $5 million in cybersecurity coalition," Target Corporation website, https://corporate.target.com/article/2014/02/target-to-invest-5-million-in-cybersecurity-coalit, accessed May 4, 2016.

[61] Target Corporation, "A message from CEO Gregg Steinhafel about Target's payment card issues," Target Corporation website, https://corporate.target.com/article/2013/12/important-notice-unauthorized-access-to-payment-ca, accessed May 4, 2016.

[62] Eric Weibel, "Target Data Breach highlights need for businesses to purchase cyber insurance," *Examiner*, December 21, 2013.

[63] Target Corporation, "A message from CEO Gregg Steinhafel about Target's payment card issues."

[64] Ibid.

[65] Meagan Clark, "Timeline of Target's Data Breach And Aftermath: How Cybertheft Snowballed For The Giant Retailer."

[66] Target Corporation, "A message from CEO Gregg Steinhafel about Target's payment card issues."

[67] Ibid.

[68] Ibid.

[69] Aimee Picchi, "Customers seeing red over Target's hacking response," *MoneyWatch*, December 20, 2013.

[70] Brian Krebs, "Cards Stolen in Target Breach Flood Underground Markets," *Krebs on Security* (blog), December 20, 2013.

[71] Ibid.

[72] Jim Finkle and David Henry, "Exclusive: Target hackers stole encrypted bank PINs—source," Reuters, December 25, 2013.

[73] David Goldman, "Target confirms PIN data was stolen in breach," CNN Money, December 27, 2013.

[74] *Amalgamated Bank v. Target Corporation*, No. 14-cv-00263-DWF-SER, Complaint (D. Minn. filed Jan. 28, 2014).

[75] David Goldman, "Target confirms PIN data was stolen in breach."

[76] Meagan Clark, "Timeline of Target's Data Breach And Aftermath: How Cybertheft Snowballed For The Giant Retailer."

[77] Maggie McGrath, "Target Data Breach Spilled Info On As Many As 70 Million Customers," *Forbes*, January 10, 2014.

[78] *Kulla v. Steinhafel*, No 0:14-cv-00203, Complaint (D. Minn. filed Jan 21, 2014).

[79] Hadley Malcolm, "Target: Data stolen from up to 70 million customers," *USA Today*, January 10, 2014.

[80] Aimee Picchi, "After security breach, Target's brand takes a hit," *CBS Money Watch*, December 27, 2013.

[81] Becky Quick and Matthew J. Belvedere, "Target CEO 'still shaken' by the data breach, vows to 'make it right.'"

[82] Sara Germano, Robin Sidel, and Danny Yadron, "Target Faces Backlash After 20-Day SecurityBreach," *Wall Street Journal* Online, December 19, 2013.

[83] In re: Target Corp. Customer Data Security Breach Litigation, No 0:14-md-02522, Complaint (D. Minn. filed Aug. 25, 2014).

[84] Danny Yadron, Paul Ziobro, and Devlin Barrett, "Target Warned of Vulnerabilities Before Data Breach," *Wall Street Journal*, February 14, 2014.

[85] Senate Committee on Commerce, Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach,* 113th Cong., 2nd sess., 2014.

[86] Danny Yadron et al., "Target Warned of Vulnerabilities Before Data Breach."

[87] Target Corporation, "Testimony of John Mulligan," Target Corporation website, https://corporate.target.com/_media/TargetCorp/global/PDF/Target-SJC-020414.pdf, accessed May 26, 2016.

[88] Jennifer Bjorhus, "Clean reviews preceded Target's data breach, and others," *Star Tribune*, March 31, 2014.

[89] Kim Zetter, "Will Target's Lawsuit Finally Expose the Failings of Security Audits," *Wired*, March 28, 2014.

[90] Ibid.

[91] Ibid.

[92] Ibid.

[93] Ibid.

[94] Jennifer Bjorhus, "Clean reviews preceded Target's data breach, and others."

[95] Ibid.

[96] In re: Target Corp. Customer Data Security Breach Litigation, No 0:14-md-02522, Complaint (D. Minn. filed Aug. 25, 2014).

[97] Senate Committee on Commerce, Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach*, 113th Cong., 2nd sess., 2014.

[98] Target Corporation, "Segment total sales: percentage change from prior year," Target Corporation website, http://investors.target.com/phoenix.zhtml?c=65828&p=irol-summaryfinancial, accessed May 26, 2016.

[99] Elizabeth A. Harris, "Data Breach Hurts Profit at Target," *New York Times*, February 26, 2014.

[100] Data from Capital IQ.

[101] Kevin M. McGinty, "Target Data Breach Price Tag: $252 Million and Counting," *Privacy and Security Matters*, February 26, 2015.

[102] Kaleigh Simmons, "Everything you need to know about the Target data breach lawsuits," *Rippleshot*, February 4, 2015.

[103] Jay Rockefeller IV, "Rockefeller: Staff Report Details Target's Missed Opportunities to Stop Massive Data Breach," *Votesmart*, March 25, 2014.

[104] TGB Security, "Target CFO Grilled in Senate Hearing," TGB Security website, https://tbgsecurity.com/target-cfo-grilled-in-senate-hearing-bankinfosecurity/, accessed May 6, 2016.

[105] Elizabeth A. Harris, "Target Had Chance to Stop Breach, Senators Say," *New York Times*, March 26, 2014.

[106] D. Skariachan and J. Finkle, "Target meets with state attorneys as lawsuits pile up," Reuters, December 23, 2013.

[107] Jeffrey Roman, "Target CFO Grilled in Senate Hearing," *Bank Info Security*, March 27, 2014.

[108] Jim Spencer and Jennifer Bjorhus, "Target missed multiple data breach warnings, Senate report says," *Star Tribune*, March 27, 2014.

[109] *Davis v. Steinhafel*, No. 0:14-cv-00203, Brief (D. Minn. filed May 8, 2014).

[110] Gregory Wallace and Gabrielle Solomon, "Black Thursday? Thanksgiving sales numbers growing," CNN Money, November 30, 2014.

[111] In re: Target Corp. Customer Data Security Breach Litigation, No 0:14-md-02522, Complaint (D. Minn. filed Aug. 25, 2014).

[112] Cryptography Fundamentals, "Target," Cryptography Fundamentals website, http://cryptofundamentals.com/target, accessed May 27, 2016.

[113] In re: Target Corp. Customer Data Security Breach Litigation, No 0:14-md-02522, Complaint (D. Minn. filed Aug. 25, 2014).

[114] Ibid.

[115] Keller Rohrback, "Target Data Breach," Keller Rohrback website, http://krcomplexlit.com/currentcases/target-data-breach/, accessed May 7, 2016.

[116] Y. Peter Kang, "Target's $10M Deal Over Data Breach Gets Final Approval," *Law360*, November 17, 2015.

[117] In re: Target Corp. Customer Data Security Breach Litigation, No 0:14-md-02522, Complaint (D. Minn. filed Aug. 25, 2014).

[118] Jim Finkle and Mark Hosenball, "Exclusive: More well-known U.S. retailers victims of cyber attacks—sources."

[119] Ibid.

[120] Ibid.

[121] In re: Target Corp. Customer Data Security Breach Litigation, No 0:14-md-02522-PAM, Declaration of Charles S. Zimmerman (D. Minn. filed Dec. 2, 2015).

[122] *Amalgamated Bank v. Target Corporation*, No. 14-cv-00263-DWF-SER, Complaint (D. Minn. filed Jan. 28, 2014).

[123] Ibid.

[124] Jonathan Stempel and Nandita

Bose, "Target in $39.4 million settlement with banks over data breach," Reuters, December 2, 2015.

[125] In re: Target Corp. Customer Data Security Breach Litigation, No 0:14-md-02522-PAM, Declaration of Charles S. Zimmerman (D. Minn. filed Dec. 2, 2015).

[126] *Amalgamated Bank v. Target Corporation*, No. 14-cv-00263-DWF-SER, Complaint (D. Minn. filed Jan. 28, 2014).

[127] Matthew Heller, "Survey Shows Toll of Target Breach on Banks," *CFO* website, http://ww2.cfo.com/fraud/2014/09/survey-shows-toll-target-breach-banks/, accessed May 7, 2016.

[128] Tracy Kitten, "Target Breach: MasterCard Weighs New Settlement," *Bank Info Security*, August 20, 2015.

[129] Jonathan Stempel and Nandita Bose, "Target in $39.4 million settlement with banks over data breach."

[130] Ibid.

[131] *Davis v. Steinhafel*, No. 0:14-cv-00203, Brief (D. Minn. filed May 8, 2014).

[132] *Kulla V. Steinhafel*, No 0:14-cv-00203, Complaint (D. Minn. filed Jan. 21, 2014).

[133] Ibid.

[134] Ibid.

[135] Ibid.

[136] Ibid.

[137] *Davis V. Steinhafel*, No 0:14-cv-00261, Complaint (D. Minn. filed Jan. 28, 2014).

[138] Ibid.

[139] *Davis v. Steinhafel*, No. 0:14-cv-00203, Brief (D. Minn. filed May 8, 2014).

[140] Target Corporation, "Audit and Finance Committee Charter," Target Corporation website, http://investors.target.com/phoenix.zhtml?c=65828&p=irol-govcommittees, accessed May 11, 2016.

[141] Ibid.

[142] Donna Dabney, "Did ISS get it right in recommending a vote against Target's directors?," The Conference Board website, http://tcbblogs.org/governance/2014/06/04/did-iss-get-it-right-in-recommending-a-vote-against-targets-directors/, accessed May 7, 2016.

[143] Ibid.

[144] "Target Corporation Proxy Statement and Notice of Annual Meeting of Shareholders," SEC Filing, May 19, 2014, accessed, May 7, 2016.

[145] Target Corp., 2012 10-K, p. 7, https://corporate.target.com/_media/TargetCorp/annualreports/content/download/pdf/Annual-Report.pdf?ext=.pdf.

[146] "Target Corporation," ISS Proxy Advisory Services, May 27, 2014.

[147] Ibid.

[148] Ibid.

[149] Ibid.

[150] Ibid.

[151] Ibid.

[152] Ibid.

[153] "Proxy Paper—Target Corporation," Glass Lewis & Co., May 27, 2014.

[154] Ibid.

[155] Nick Halter, "Target chairwoman defends board's handling of data breach," *Minneapolis/St. Paul Business Journal* Online June 2, 2014.

[156] Ibid.

[157] Donna Dabney, "Did ISS get it right in recommending a vote against Target's directors?"

[158] Wayne Hood and Shannon Coyne, "Target: Comments follow Sell-Side Analyst Meeting," BMO Capital Markets, June 2, 2014.