EXHIBIT B

TARGET CORPORATION

REPORT OF THE SPECIAL LITIGATION COMMITTEE

MARCH 30, 2016

EXECUTIVE SUMMARY

In the three week period between November 27 and December 18, 2013, Target Corporation experienced a data breach in which a hacker stole the payment card data of up to 40 million of its customers and stole personally identifiable information—specifically names, residence addresses, phone numbers, and/or email addresses—of up to 70 million of its customers. The announcement of the breach led to widespread media attention, negatively affected Target's sales, and had an immediate and detrimental effect on Target's reputation with consumers. As a result, congressional committees sought testimony and information from Target, regulatory agencies began investigations, and private litigants initiated claims.

Among those private litigants were six Target shareholders. One made a derivative demand on Target's Board of Directors that it investigate and bring actions against the Board members and the company's CEO, CFO, and CIO. The others sued the Board members and officers in five derivative lawsuits. Four of the lawsuits were brought in United States District Court for the District of Minnesota and were ultimately consolidated. One was brought in Hennepin County District Court for the State of Minnesota.

The crux of the claims made in the demand and the lawsuits is twofold: that Target's officers and directors—in conscious disregard of their duties—breached their fiduciary duties to Target by 1) failing to oversee Target's information security program and 2) failing to give its customers prompt and accurate information in disclosing the breach.

In response to the derivative lawsuits and demand, Target's Board of Directors formed this Special Litigation Committee (the "SLC") composed of two Minnesota jurists—Chief Justice Kathleen Blatz, ret., and Professor John Matheson. The SLC's members were not Target Board members and did not have any material connections to Target, its officers, or its Board of

Directors. The Board invested the SLC with complete power and authority over this matter, including the unrestricted power to investigate and evaluate the claims made against the officers and directors, to determine whether and to what extent it would be in Target's best interests to pursue any of the claims raised by any of the shareholders, and to respond to the shareholders' demand and lawsuits.

Over a period of twenty-one months, the SLC investigated and evaluated the claims made in the demand and derivative complaints. During that time, with the assistance of independent counsel, it searched databases containing hundreds of thousands of documents, reviewed thousands of documents, interviewed 68 witnesses, received information and opinions from independent experts it hired, considered the applicable law, and deliberated. In its deliberations, the SLC considered whether valid legal claims exist; it also undertook a comprehensive weighing and balancing of the legal, ethical, commercial, professional, public relations, fiscal, and other factors common to reasoned business decisions in deciding whether it would be in Target's best interests to pursue claims against the officers and directors named in the demand letter and derivative complaints. The SLC has concluded that it is not in Target's best interests to pursue such claims.

Consequently, under the plenary power granted by Target's Board of Directors, the SLC will notify the shareholder who made the demand that Target will not pursue an action against current and former directors and officers. The SLC also will seek the dismissal of the derivative cases pending in state and federal court.

I. Target Corporation History

In May of 1961, the Dayton Company, a department store retailer incorporated in Minnesota in 1902, announced its plans to form a new discount chain store. Approximately one year later, on May 1, 1962, Dayton's opened its first Target store in Roseville, Minnesota. By the end of 1962, three additional Target stores had been opened in St. Louis Park, Crystal, and Duluth. In 1966, the first Target store outside of Minnesota was opened in the Denver metro area. Meanwhile, Dayton's had itself become a national retailer; and, on October 18, 1967, Dayton Corporation's stock went public.

Two years later, Dayton Corporation acquired J.L. Hudson Company and became the Dayton-Hudson Corporation. By 1979, Target Stores, one of the Dayton-Hudson Corporation's five autonomous divisions, reached $1 billion in annual sales. In 1990, Dayton-Hudson purchased Marshall Field & Company, a Chicago-based department store, making Dayton-Hudson the largest department store company in the Midwest. By 2000, the Target Stores' revenues and profits had eclipsed those of the department stores; and, on January 30, Dayton-Hudson Corporation changed its name to Target Corporation.

Meanwhile, Target launched its first store credit card, known as the Target Guest Card, in 1995. Target followed in 2001 with the Target Visa® Credit Card, the first company credit card to be accepted at major retailers nationwide. Renamed REDcards in 2004, the portfolio of credit products was expanded to add the Target Check Card in 2007.

Today, Target Corporation, headquartered in Minneapolis, Minnesota, is a Fortune 50 company. Target is the nation's sixth largest retail company with sales of $73.8 billion for the fiscal year ending January 2016. As of January 30, 2016, Target employed approximately

341,000 people,[1] operated approximately 1,800 stores in the United States, and had 38 distribution centers in the United States.

II. Target's Data Breach and Customer Notification

On November 12, 2013, a hacker entered Target's system using credentials that it stole from one of Target's HVAC and refrigeration vendors. The hacker installed malware on Target's United States point-of-sale registers and stole payment card data for up to 40 million credit and debit card accounts of customers who shopped at Target's United States brick-and-mortar stores between November 27 and December 18, 2013. The hacker did not obtain payment card data from individuals who shopped only at Target Canada stores or on Target.com during the period.

The hacker was also able to access a database that contained the names, email addresses, phone numbers, and/or physical addresses of up to 70 million Target shoppers and was able to extract that information as well.

A. Discovery of the Data Breach

On December 12, 2013, the United States Department of Justice notified Target that it had discovered the black market sale of large batches of payment cards whose common denominator was that they had been used at Target stores. Target immediately began investigating its systems to determine whether they had been compromised. Target representatives met with the Department of Justice and the Secret Service on December 13, 2013. Target senior executives were notified of the potential issue later that evening.

On December 15, 2013, Target confirmed internally that a hacker had infiltrated its network, installed malware on over 40,000 of its point-of-sale registers, and extracted customer

[1] Employment levels peaked at roughly 390,000 employees during the 2015 sales period from Thanksgiving to the end of December.

payment card data. The malware installed by the hacker captured payment card data from the magnetic strip of cards immediately after a card was swiped but before Target's system encrypted the data. On December 15, within twelve hours after they identified the malware, Target's forensic personnel removed the malware from almost all of the registers.[2] On December 18, Target disabled the malware on the remaining registers.

Although the hacker captured the information contained on the magnetic strip of both credit and debit cards, debit-only cards cannot be used without the associated PIN data. Although the hacker was able to remove PIN data, the data had been encrypted and the encryption key required to decrypt it could not be accessed through Target's network. Because the PIN data was encrypted, Target notified the public and its customers that the debit card accounts themselves were not compromised. The Target breach has not led to increased fraud on those debit cards.

During its investigation, Target also discovered that the hacker had stolen, in addition to payment card data, personal information of a large number[3] of Target customers contained in an internal Target database. The information extracted included customers' names, phone numbers, email addresses, and/or physical addresses. It did not include driver's license data, social security numbers, credit scores, pharmaceutical information, or health information.

---

[2] Approximately 25 registers were offline from Target's system when the initial malware removal took place on December 15 and thus were not secured until December 18. Payment card data used in transactions made by 56 customers during December 16 and December 17 was stolen prior to Target's disabling the malware on one of those remaining registers.

[3] The hacker stole approximately 70 million records from the database. Because many records were old, duplicative, or otherwise incorrect, Target does not know exactly how many individuals from this database had their information compromised. Target's Board of Directors and Target management ultimately chose to disclose that up to 70 million customers' information was potentially compromised because that number had been determined to be the logical maximum.

Target senior management and members of the Executive Committee were provided updates in real-time and continued to evaluate the situation by meeting several times a day in the period immediately following the discovery of the breach. Management notified the Board of Directors of the data breach on December 18. Thereafter, management kept the members of its Board of Directors apprised of developments with daily emails and frequent telephone calls.

B. Customer Notification of the Data Breach

On December 15, after Target had internally confirmed the existence of malware designed to capture payment card data on store registers and had removed most of the malware from the registers, management began preparing to notify the public of the breach. Although its investigation was incomplete and ongoing, Target management knew that a large number of payment cards had been stolen and knew that Target would have to make a large number of important communications regarding the data breach. While management's goal was to have Target make timely, truthful, and transparent disclosures, management believed it would be harmful to make a public disclosure before Target was prepared. From December 15 through December 18, Target's actions included gathering accurate details about the breach, sending contractually required alerts to payment processors and card networks, expanding Target's ability to notify customers through its call centers and guest service and registry departments, retaining legal counsel to prepare for potential litigation, and working with legal counsel to ensure Target was complying with the laws of forty-seven states and the District of Columbia governing data breach notification. Target also collaborated with the Secret Service and other authorities to assist those authorities in their investigations and engaged a third-party firm to perform an independent forensic investigation of the breach as required by Target's agreements with the payment card networks.

From the time it was first notified of the breach, the Board encouraged management to make early public disclosure. The Board's position on early disclosure was taken despite the uncertainty surrounding some factual details and despite Target's not having completed all preparations.

On the afternoon of December 18, while Target was preparing to notify the public of the breach, a cybersecurity blogger named Brian Krebs made the first public report that Target had been breached. A number of major media outlets picked up on Krebs's report.

The next day, Target provided broad public notice of the breach on its website, through the media, and by using social media outlets. In addition to broad public disclosure, on December 19 and 20, Target also directly notified roughly 17 million customers by email. Target also provided its REDcard holders with additional information relating to their cards in emails sent on December 23 and 24.

As soon as the news hit, customers started calling Target. At peak, Target was fielding calls from approximately 50,000 people per hour.

Target continued its forensic investigation while updating the public with relevant information. On January 9, 2014, Target's investigation confirmed that the hacker, in addition to stealing payment card data, had also taken customers' personal information. The next day, Target notified the public of its discovery that up to 70 million of those customer records had been stolen. Target made the information available on its website and also sent notices by email. In providing notification, Target again sought to comply with all forty-seven states' laws as well as those of the District of Columbia.

In its communications, Target offered all customers who had ever shopped in United States stores one year of free credit monitoring and identity-theft protection. Approximately 2.5 million customers redeemed the offer.

III. Derivative Lawsuits and Demand[4]

A. Derivative Lawsuits

1. Shareholder Derivative Actions in Federal Court

a. Individual Federal Derivative Complaints

Shortly after Target issued its initial press release confirming the data breach, shareholder Robert Kulla filed the first shareholder derivative suit arising out of the data breach in United States District Court for the District of Minnesota. Kulla's suit was brought against Target Board members and certain officers and sought corporate changes and damages. Three other federal derivative complaints soon followed.[5]

All four shareholders named as defendants Gregg W. Steinhafel, Target's Chairman, Chief Executive Officer, and President, and Beth M. Jacob, its Chief Information Officer, along with the entire Board of Directors at the time of the breach: James A. Johnson, Solomon D. Trujillo, Anne M. Mulcahy, Roxanne S. Austin, Calvin Darden, Mary E. Minnick, Derica W. Rice, John G. Stumpf, Douglas M. Baker, Jr., Henrique De Castro, and Kenneth L. Salazar. Two of the shareholders, Maureen Collier and the Police Retirement System of St. Louis, also named

[4] The operative shareholder complaints as filed are attached at Appendix A. The demand letters are attached at Appendix B. Although summarized in this report, the SLC read and considered the demand letters and the complaints in their entirety.

[5] *Kulla v. Steinhafel, et al.*, 14-cv-203 (PAM/JJK), filed Jan. 21, 2014;
Davis v. Steinhafel, et al., 14-cv-261 (PAM/JJK), filed Jan. 28, 2014;
Collier v. Steinhafel, et al., 14-cv-266 (PAM/JJK), filed Jan. 29, 2014; and
The Police Retirement System of St. Louis v. Steinhafel, 14-cv-551 (PAM/JJK), filed Feb. 27, 2014.

John J. Mulligan, Target's Chief Financial Officer, as an individual defendant. All shareholders, as is procedurally required, named Target as a nominal defendant.

Three of the complaints, those of Kulla, Davis, and the St. Louis Police Retirement System, are all but identical (the "Kulla complaints"), although the St. Louis Police Retirement System's complaint differs in that it added a specific claim against the members of the Audit Committee and also added a number of factual allegations. The Kulla Complaints and Collier all generally alleged that the officer and director defendants (1) caused or allowed Target to have inadequate controls over the information security program and (2) caused or allowed Target to make untimely or misleading public disclosures that concealed the full scope of the breach.

The complaints contained allegations that the individual defendants, by causing or allowing the data breach, breached their fiduciary duties of good faith, due care, and loyalty. Collier also added claims of breach of the duties of oversight, fair dealing, and candor and included a cause of action for gross mismanagement and abuse of control. All the initial complaints alleged that the individual defendants wasted corporate assets and all sought cash payment[6] from the individual defendants and reformation of internal controls, policies, and practices.

b. Consolidated Shareholder Complaint

On April 14, 2014 the Court ordered the consolidation of the four federal derivative cases.[7] On July 18, three of the derivative shareholders filed their consolidated complaint.[8] That consolidated complaint generally alleged that the individual defendants wasted corporate assets

[6] The cash demand was for money damages, restitution, or both.
[7] *Davis, et al. v. Steinhafel, et al.*, 14-cv-00203 (PAM/JJK).
[8] Kulla was no longer a named plaintiff as of July 21, 2014.

and breached their fiduciary duties of loyalty, good faith, and due care through wrongful acts and omissions, including the following:

- failing to "implement and oversee the people, policies, and procedures" necessary to successfully run Target's data security program;
- failing to ensure Target had formal data security risk management guidelines, policies, and procedures in place and failing to monitor or oversee any such systems that were in place;
- failing to establish and monitor an adequate corporate governance system to address data security issues;
- ignoring red flags, including published papers on security threats and a 2007 attack on Target's computer systems;
- failing to ensure that Target followed standard information technology practices;
- failing to put the proper people in the proper positions to manage data security risks;
- failing to ensure that Target complied with applicable industry standards, laws, and regulations;
- failing to direct the company to timely and adequately notify the public of the breach, both in the company's initial and ongoing breach communications; and
- conspiring with or aiding and abetting one another to disguise the violations of law, breaches of fiduciary duties, and waste of corporate assets previously alleged.

The shareholders claim that as a result of those failures Target suffered substantial damages, including lost revenue and profit, investigation expenses, capital expenses due to a credit downgrade, costs incurred as a result of class action lawsuits brought by financial institutions and consumers, and payments of compensation and benefits to individual defendants who breached their fiduciary duties.

The consolidated complaint pleads the causes of action in two counts. Count I sets out claims against the officers and, separately, the directors. The officers, it is alleged, breached their fiduciary duties of loyalty and care by knowingly or in conscious disregard of their duties (1) failing to implement a system of internal controls to protect customers' information; (2)

failing to oversee the inadequate controls; and (3) causing the company to conceal the full scope of the breach. The directors are alleged to have breached their duty of loyalty[9] by making the same mistakes with the same state of mind.

Count II of the consolidated complaint alleges a cause of action for waste of corporate assets. Plaintiffs allege the waste included: (1) failing to implement controls to prevent the breach causing the attendant losses and expenses; and (2) paying salaries and bonuses to the officers and directors who breached their fiduciary duties.

The relief sought in the amended complaint is that the individual defendants be ordered to pay monetary damages and restitution and that the Board and officers be ordered to reform corporate governance policies and internal procedures to protect the Company and its shareholders from another breach.

The action was stayed on June 23, 2014 pending the outcome of the SLC's investigation and report.

2. ***Shareholder Derivative Action in State Court***

On February 6, 2014, shareholder Beth Koeneke filed a shareholder derivative lawsuit in Hennepin County District Court for the State of Minnesota against the eleven Target directors named in the federal suits, two Target officers (Steinhafel and Jacob), and Target as the nominal defendant.[10]

---

[9] Although in the early paragraphs of the consolidated complaint it is alleged that the officers and directors breached the duties of loyalty, good faith, and due care, in the count of the consolidated complaint separately setting forth the claim of breach of fiduciary duty, neither the officers nor the directors are charged with a lack of good faith and the directors are not charged with a lack of due care.

[10] *Koeneke v. Austin, et al.*, Case No. 27-cv-14-1832.

Koeneke generally alleged, like the federal derivative shareholder plaintiffs, that the individual defendants failed to implement a system of internal controls, policies, and procedures for the protection of customer data, failed to monitor those systems, and failed to direct Target to promptly and accurately notify its customers about the data breach. She alleged three causes of action: (1) a knowing, willful, or grossly negligent breach of the duty of loyalty; (2) the commission of corporate waste; and (3) abuse of control. She too sought money damages and corporate reforms.

In response to Koeneke's complaint, on April 11, 2014, Target moved to stay the action, or, in the alternative, to dismiss it. Target alleged that Koeneke failed to make a pre-suit demand on the Board and her complaint failed to state a claim for which relief could be granted. The parties stipulated that the action be stayed pending the outcome of the related federal cases, and, on May 21, 2014, the Court granted the stay.

B. Shareholder Demand

On April 10, 2014, counsel for a sixth shareholder, the Paul Perry Revocable Living Trust (the "Trust"), wrote to Steinhafel in his capacity as Target's Chairman of the Board, Chief Executive Officer, and President (the "Demand"). The Trust demanded that the Board commence litigation against the Board members and three officers, including Steinhafel himself. The Trust alleged that those individuals had breached their fiduciary duties of good faith, loyalty, and due care by, among other things, consciously disregarding red flags regarding data security risks, directing Target to inadequately and improperly communicate with customers regarding the data breach, failing to establish and maintain adequate internal controls, and causing the issuance of misleading financial statements. The Trust specifically criticized members of the Board's Audit Committee because it was charged with (1) ensuring Target complied with legal

and regulatory requirements, (2) monitoring Target's internal controls, and (3) overseeing Target's risk management practices.

The Trust alleged that these and other failures led Target to incur substantial damages. The Trust requested that the Board undertake an internal investigation into the alleged violations and commence a civil action against the identified individuals to recover damages for Target.

On May 21, 2014, counsel sent a supplemental letter on behalf of the Trust, which added the following requests to its Demand: (1) that the Board deny Steinhafel severance benefits after his resignation; and (2) failing that, that the Board and Steinhafel enter into a standstill agreement (or "freeze") to hold payment of his severance benefits in abeyance during the investigation of the Demand and the resulting legal action, if any. The Trust further requested that any benefits already provided to Steinhafel be returned to Target immediately.

C. Individual Defendants

1. Director Defendants

The current and former directors listed below are named in the Demand and in each of the shareholder derivative complaints.

Roxanne S. Austin has served on Target's Board of Directors since 2002. At various times during her tenure, Austin has been a member of Target's Governance Committee, Finance Committee, and Audit Committee. She chaired the Audit Committee for approximately ten years. She currently chairs the Infrastructure and Investment Committee and serves on Target's Audit and Finance Committee and its Risk and Compliance Committee. From May to August 2014, Austin held the position of the interim Chair of Target's Board of Directors. When she joined the Target Board, Austin was President and Chief Operating Officer of DIRECTV, Inc., a position she held from June 2001 to December 2003. Since then, Austin has served as President

of Austin Investment Advisors, a private investment and consulting firm. Austin began her career at Deloitte & Touche LLP after earning a bachelor's degree in accounting from the University of Texas at San Antonio in 1982. Currently, Austin also serves on the boards of Abbott Laboratories, AbbVie Inc., Teledyne Technologies Incorporated, and LM Ericsson Telephone Company.

Douglas M. Baker, Jr. joined Target's Board of Directors in March 2013. He has served on Target's Audit Committee, Nominating and Governance Committee, and Compensation Committee. He is currently a member of the Human Resources and Compensation Committee and the Nominating and Governance Committee. Baker is Target's Lead Independent Director. After earning an undergraduate degree from the College of the Holy Cross in Worcester, Massachusetts in 1981, Baker joined Proctor & Gamble, where he worked until he joined Ecolab, Inc. in 1989. Ecolab is a Fortune 500 company that focuses on providing water, hygiene, and energy technologies and services. Baker became Ecolab's Chief Executive Officer in July 2004 and Chairman of its Board in May 2006. He also serves on the board of U.S. Bancorp.

Calvin Darden has served on Target's Board of Directors since 2003. At various times during his tenure on the Board, Darden has been a member of the Compensation Committee, the Nominating and Governance Committee, and the Corporate Responsibility Committee. Darden presently serves on the Human Resources and Compensation Committee and the Nominating and Governance Committee. Darden began his career at United Parcel Service, Inc. (UPS) as a part-time package handler in 1971. He worked there while earning a Bachelor of Science in business administration from Canisius College in Buffalo, New York. After graduating, Darden joined UPS as a full-time employee. He then held a number of positions at UPS, ultimately becoming

Senior Vice President of U.S. Operations. Darden held that position from January 2000 until his retirement in 2005. Since 2005, Darden has held positions as Chairman of The Atlanta BeltLine, Inc. and Darden Development Group, LLC. He is currently Chairman of Darden Putnam Energy & Logistics, LLC. Darden also currently serves on the boards of Cardinal Health, Inc. and Coca-Cola Enterprises.

Henrique De Castro joined Target's Board of Directors in March 2013. He has served on Target's Corporate Responsibility Committee, Nominating and Governance Committee, and Finance Committee. De Castro presently is a member of the Human Resources and Compensation Committee and the Infrastructure and Investment Committee. At the time he joined the Target Board, De Castro was serving as Chief Operating Officer of Yahoo! Inc. He held that position from November 2012 to January 2014. Before that, he worked for Google, Inc. in a number of roles, including, from March 2012 to November 2012, as President of Partner Business Worldwide; from June 2009 to March 2012, as President of Global Media, Mobile & Platforms; and from July 2006 to May 2009, as Managing Director of European Sales. Originally from Portugal, De Castro earned a degree in business administration from the University of Lisbon and an M.B.A. from the International Institute for Management Development in Lausanne, Switzerland.

James A. Johnson served on Target's Board of Directors from 1996 until his retirement in June 2015. Johnson was a member of the Corporate Responsibility Committee for nearly all of his twenty-year tenure. He also served on the Compensation, Finance, and Governance Committees, all of which he chaired at some point. Johnson served as Target's Lead Independent Director from 2005 until March 2015. He retired from the Board three months later, in June 2015. Shortly before retiring, Johnson chaired the Compensation Committee and

served on the Corporate Responsibility Committee. Johnson earned a degree in political science from the University of Minnesota in 1966 and a Master of Public Affairs from the Woodrow Wilson School at Princeton University in 1968. Johnson then held a variety of governmental/political positions and is a former CEO of Federal National Mortgage Association (Fannie Mae). In 2000, Johnson founded Johnson Capital Partners, a private consulting company, and remains its chairman. Johnson was also Vice Chairman of Perseus, LLC, a merchant-banking private-equity firm, from April 2001 to June 2012. Johnson currently serves as a director at Goldman Sachs Group, Inc.

Mary E. Minnick has been a director since 2005. She served on the Corporate Responsibility Committee from 2006 through 2014 and has also served on the Finance, Governance, and Audit Committees at various times. Minnick presently sits on both the Audit and Finance Committee and the Infrastructure and Investment Committee. At the time of her election to the Board, Minnick was an Executive Vice President and the President of Marketing, Strategy, and Innovation for the Coca-Cola Company. She worked at Coca-Cola for 23 years. Minnick joined Coca-Cola after earning an undergraduate degree from Bowling Green State University in 1981 and an M.B.A. from Duke University in 1983. In May 2007, Minnick left Coca-Cola and became a partner in Lion Capital LLP, a London-based private equity firm, where she remains today. In addition to serving on Target's Board of Directors, Minnick also serves on the boards of The Heineken Company and The WhiteWave Foods Company.

Anne M. Mulcahy has served on Target's Board of Directors since 1997 and has served on its Finance Committee, Corporate Responsibility Committee, Audit Committee, and Nominating and Governance Committee. Her tenure includes time chairing the Nominating and Governance and the Finance Committees. Mulcahy currently serves on the Human Resources

and Compensation Committee (which she chairs), the Nominating and Governance Committee, and the Risk and Compliance Committee. Mulcahy spent most of her career at the Xerox Corporation. Mulcahy joined Xerox in 1976 after earning an undergraduate degree from Marymount Manhattan College, volunteering for Teach for America, and working for Chase Manhattan Bank. Mulcahy held a number of positions at Xerox, ultimately becoming Chief Executive Officer, a position she held from August 2001 to July 2009, and Chair of the Board from January 2002 to May 2010. Currently, Mulcahy serves on the boards of Graham Holdings Company, Johnson & Johnson, and LPL Financial Holdings Inc. In addition, she is currently the Chair of the Board of Trustees of Save The Children Federation, Inc.

Derica W. Rice has served on Target's Board of Directors since 2007. He has served on the Governance, Finance, and Audit Committees. Rice now chairs the Audit and Finance Committee and serves on the Risk and Compliance Committee. Rice earned a bachelor's degree in electrical engineering from Kettering University and an M.B.A. from Indiana University. He began working for Eli Lilly and Company in 1990, where he held a variety of financial and executive positions. In 2006, Rice became Eli Lilly's Chief Financial Officer. He still holds that position and is an Executive Vice President and a member of the Executive Committee there. Rice served as acting Chief Executive Officer of Eli Lilly from May 2013 to July 2013 when its permanent CEO underwent medical treatment. Rice currently serves on the boards of Indiana University and the Center for Leadership Development.

Kenneth L. Salazar joined Target's Board of Directors in July 2013. Upon joining the Board, Salazar became a member of the Corporate Responsibility and the Nominating and Governance Committees. He currently chairs the Risk and Compliance Committee and serves on the Infrastructure and Investment Committee. Salazar earned an undergraduate degree from

Colorado College in 1977 and a law degree from the University of Michigan in 1981. Salazar served as the Attorney General for the State of Colorado from 1999 until 2005; as a United States Senator from Colorado from January 2005 until January 2009; and as the United States Secretary of the Interior from January 2009 until 2013. Salazar has also worked in the private practice of law for a number of years and is currently employed as a partner at the law firm of Wilmer Cutler Pickering Hale and Dorr LLP.

John G. Stumpf has served on Target's Board of Directors since March 2010. Since joining the Board, Stumpf has served on the Finance, Compensation, and Audit Committees. He currently serves on the Risk and Compliance Committee, the Audit and Finance Committee, and the Nominating and Governance Committee, which he chairs. When he joined the Target Board, Stumpf was Wells Fargo's Chairman of the Board, President, and Chief Executive Officer. Stumpf had joined the Norwest Corporation, a predecessor to Wells Fargo & Company, in 1982 after he had earned an undergraduate finance degree from St. Cloud State University and an M.B.A. from the Carlson School of Management at the University of Minnesota. Stumpf held a variety of positions at Norwest, and later Wells Fargo, ultimately rising to his present position at Wells Fargo. Stumpf also serves on the board of the Chevron Corporation.

Solomon D. Trujillo served on Target's Board of Directors from 1994 until his retirement in March 2014. At the time of his retirement, Trujillo had been the chair of Target's Corporate Responsibility Committee for nearly ten years and was on the Nominating and Governance Committee. During his tenure, Trujillo also served on the Compensation, the Finance, and the Nominating and Governance Committees. Trujillo earned both a bachelor's degree in business and an M.B.A. from the University of Wyoming. Upon graduating, Trujillo began working in the telecommunications industry. Trujillo has held positions as the Chief

Executive Officer of U.S. West, Orange S.A., and Telstra Corporation Limited, telecommunications service providers respectively located in the United States, France, and Australia. Trujillo currently serves as a director for WPP plc.

2. ***Officer Defendants***

The current and former officers listed below are named in the Demand and the consolidated shareholder complaint.

Gregg W. Steinhafel joined Target after obtaining an undergraduate degree from Carroll University in 1977 and an M.B.A. from the Kellogg School of Management at Northwestern in 1979. Steinhafel held a variety of merchandising positions at Target and became the Executive Vice President of Merchandising in 1994. In that position, Steinhafel worked with Target's then CEO, Bob Ulrich, to enhance Target's branding efforts. In May 2008, Ulrich stepped down and Steinhafel became President and Chief Executive Officer. Steinhafel added the title of Chairman of the Board in February 2009, and served as President, CEO, and Chairman until his resignation in May 2014. Following Steinhafel's resignation, he and Target entered into an agreement whereby he would continue to serve Target in an advisory capacity until August 2014. Steinhafel was not a director or officer during this advisory period. Steinhafel currently serves on the board of The Toro Company.

John J. Mulligan joined Target in 1996 as a financial analyst. Before starting his career at Target, Mulligan received an undergraduate degree in electronics and electrical engineering from the University of Wisconsin-Madison in 1988 and worked for Kimberly Clark as an engineer and manager. Mulligan then obtained an M.B.A. from the Carlson School of Management at the University of Minnesota in 1996. Mulligan subsequently joined Target, where he held a variety of financial planning and analytical positions. Mulligan became Target's

Chief Financial Officer in 2012 and remained CFO until he was promoted to the newly-created position of Chief Operating Officer, effective September 1, 2015. As Target's CFO, Mulligan was responsible for the Target Information Protection team (TIP), whose data security responsibilities included implementing Target's network security policies and procedures, prioritizing security-related investments, and managing teams with various roles in Target's information security program. That team reported to the leader of Target's Financial and Retail Services business unit, who in turn reported to Mulligan. Mulligan also served as the interim President and Chief Executive Officer from the time of Steinhafel's resignation in May through August 2014. Mulligan currently serves on the board of the McDonald's Corporation.

Beth M. Jacob first joined Target in 1984 upon graduating from the University of Minnesota with a degree in retail merchandising. Two years later, Jacob moved to what is now Ameriprise Financial, Inc., where she worked in a variety of positions from 1986 to 2002. In 1989, while at Ameriprise, Jacob earned an M.B.A. from the Carlson School of Management. In 2002, Jacob left Ameriprise and began working for Target again. She held a variety of customer service roles for the Company before being promoted to Senior Vice President and Chief Information Officer (CIO) in 2008. As CIO, Jacob supervised Target Technology Services (TTS), Target's information technology function. TTS included the Security Operations Center—which monitored Target's network and responded to alerts—as well as a dedicated data security team. In 2010, during her CIO tenure, Jacob was promoted to Executive Vice President and, in 2011, gained the responsibility and title of the Head of Global Operations. Jacob resigned from Target in March 2014, three months after the data breach. In 2015, she joined SPS Commerce as Senior Vice President and Chief Customer Success Officer. Jacob currently serves on the Twin Cities Habitat For Humanity Board of Directors.

IV. Post-Breach Election of Directors

During the 2014 annual proxy shareholder voting season, Institutional Shareholder Services, Inc. (ISS), a proxy advisory firm, recommended voting against the re-election of directors serving on Target's Audit Committee and its Corporate Responsibility Committee based on those two committees' roles in risk oversight. These directors included Roxanne Austin, Calvin Darden, Henrique De Castro, James Johnson, Mary Minnick, Anne Mulcahy, and Derica Rice.[11]

In response to the adverse ISS recommendations, the Board wrote a letter to Target's shareholders discussing the Board's oversight practices and the Board's recognition of the importance of oversight responsibilities in data and cybersecurity. This letter was provided to shareholders on June 2, 2014 as additional definitive proxy soliciting materials and Rule 14(a)(12) material. ISS maintained its recommendation to vote against the same directors.

Nevertheless, all of the nominee-directors were elected for an additional term to serve on Target's Board of Directors following the 2014 shareholders' vote. The nominees received the following votes:

Nominee	**For (%)**	**Against (%)**
Roxanne Austin	78.0	22.0
Douglas Baker	95.5	4.5
Calvin Darden	79.5	20.5
Henrique De Castro	81.0	19.0

[11] Before the 2014 vote, Solomon Trujillo, who served on the Corporate Responsibility Committee, retired from the Board as required by the Corporate Governance Guidelines both because five years had elapsed since retiring from active employment and because he had reached his 20-year term limit.

James Johnson	62.9	37.1
Mary Minnick	80.0	20.0
Anne Mulcahy	63.6	36.4
Derica Rice	80.3	19.7
Kenneth Salazar	97.1	2.9
John Stumpf	94.9	5.1

The next year, at the 2015 annual shareholder meeting, all director nominees obtained above 90 percent support and all of the nominees were again re-elected for an additional term. The director nomninees received the following votes:

Nominee[12]	**For (%)**	**Against (%)**
Roxanne Austin	95.7	4.3
Douglas Baker	96.5	3.5
Brian Cornell	96.7	3.3
Calvin Darden	97.7	2.3
Henrique De Castro	98.7	1.3
Mary Minnick	98.8	1.2
Anne Mulcahy	94.0	6.0
Derica Rice	99.2	0.8
Kenneth Salazar	98.3	1.7
John Stumpf	96.3	3.7

[12] James Johnson retired from the Board in accordance with Target's mandatory retirement policy and did not seek re-election.

V. Related Litigation and Investigations

A. Private Litigation – Class Action Lawsuits

Over a hundred consumers brought actions against Target in response to the data breach. In addition, a class of banks and other financial institutions that issued payment cards compromised in the breach also filed suits. These lawsuits were brought in various jurisdictions and were ultimately consolidated, along with the derivative cases discussed above, into a multidistrict litigation (MDL) action for coordinated or consolidated pretrial proceedings in the District of Minnesota.[13] In the MDL, the cases were processed in three groups: two separate national class actions—one on behalf of the consumers and the other on behalf of the financial institutions—and the derivative cases. The Court appointed Karl Cambronne of Chestnut Cambronne PA to serve as Coordinating Lead Counsel over the MDL litigation as a whole and appointed lead counsel for each group of cases. The Court appointed Felipe J. Arroyo of Robbins Arroyo LLP to serve as Lead Counsel in the derivative cases. In addition, the Court appointed various liaison counsel and also executive and steering committees.

1. Federal Consumer Class Action

The consumer class contained 114 plaintiffs representing a class of Target customers across the United States. The consumer plaintiffs filed a seven-count consolidated complaint on August 25, 2014. The essence of their claims was that Target violated consumer protection laws and data breach laws of various states and the District of Columbia, violated the Minnesota Plastic Card Security Act, breached contracts on various grounds, and was unjustly enriched.

Target filed a motion to dismiss, which, on December 18, 2014, the Court granted in part and denied in part.

---

[13] *In re: Target Corporation Customer Data Security Breach Litigation*, 14-md-02522 (PAM)

On March 9, 2015, the putative consumer class representatives and Target entered into a settlement agreement. The settlement provided that Target pay $10 million to settle the claims of class members and pay service awards to class representatives. The class members were defined as "[a]ll persons in the United States whose credit or debit card information and/or whose personal information was compromised as a result of the data breach that was first disclosed by Target on December 19, 2013."[14]

The court preliminarily approved the proposed settlement on March 19, 2015. Notices of the proposed settlement were sent to more than 80 million identifiable members of the class and a final approval hearing was set. Final approval was granted on November 17, 2015.

All claims have been submitted, and the claims process is now closed. Four objectors appealed the settlement's approval. Two appeals remain pending. The attorneys for the class will receive, pending this appeal, $6.75 million for fees, costs, and expenses.

2. *Federal Financial Institution Class Action and Card Assessments*

Banks and financial institutions that issued the payment cards containing the information stolen during the breach claimed that Target was responsible for losses they experienced. Recompense was sought through two avenues: contractual card assessment procedures brought by the card brands on the card-issuers' behalf as well as the class action. The financial institutions alleged that Target allowed the data breach by failing to adequately secure its systems and consumer data and that Target should have more quickly discovered the intrusion and thwarted the breach. They further claimed that the data breach caused them fraud losses, costs to reissue cards, and increased customer service expenses.

[14] Excluded from the class were Target officers and directors, the court, and consumers who received notice and requested exclusion.

Before the breach, Target had entered into contractual agreements with individual card brands[15] and agreed that (1) Target would comply with the Payment Card Industry Data Security Standard (the "PCI DSS," discussed in detail *infra* at Part VIII.A); and (2) in the event of a major security breach, the card brands could fine Target if Target violated the substantive requirements contained in the contracts—in particular, if Target did not comply with PCI DSS. When assessed, these fines go into a fund that provides an alternative, non-judicial method to compensate financial institutions for losses incurred from breaches. While the class action was ongoing, the individual card brands were assessing Target's systems and whether they thought Target adhered to the requirements of the contracts.[16]

During the assessment process and before resolution of the class case, in August 2015, Target and Visa entered into a $67 million settlement. This amount included payments to Visa's fund as well as additional compensation. A financial institution accepting both payments released its right to recover through the MDL. This process resolved a substantial portion of Target's exposure.

On December 1, 2015, Target entered into a preliminary settlement agreement with the remaining financial institution class plaintiffs whose claims were not covered by the August agreement. Under the December settlement, Target was to pay approximately $39 million with approximately half going only to MasterCard issuers through MasterCard's ADC recovery program and approximately half going to the remaining class members, including banks who issued Discover, American Express, and JCB cards. The maximum amount class plaintiffs may seek for attorneys' fees, costs, expenses, and service fees to the class representatives is $20

[15] *E.g.*, Visa, MasterCard, American Express, and Discover.

[16] Different card brands have similar but different such processes. For example, Visa's process is called the Global Compromised Account Recovery Program (GCAR) and MasterCard's process is called the Account Data Compromise (ADC) recovery program.

million.[17] The Honorable Paul A. Magnuson preliminarily approved the December settlement on December 2, 2015 and scheduled the final approval hearing for May 10, 2016.

B. Administrative Investigations

Multiple governmental agencies investigated or are investigating the breach, including the Securities and Exchange Commission (SEC); the Federal Trade Commission (FTC); and a joint investigation by multiple states' attorneys general. In the second quarter of 2015, the SEC's Division of Enforcement Office notified Target by letter that the office had concluded its investigation and did not intend to recommend that the SEC undertake an enforcement action against Target with respect to the data breach.

C. Canadian Putative Class Action

In March 2014, Evan Zuckerman petitioned for a Canadian class action to be filed against Target in the Province of Québec, District of Montréal. Zuckerman alleges that he, a Canadian, shopped in Target stores in the United States using an American-issued credit card and suffered damages from the breach.[18] His claims are that Target did not have proper security measures and protocols in place, that Target was negligent because it did not monitor its systems adequately, that Target's credit monitoring offer was inadequate, and that Target failed to promptly and accurately notify all Canadian customers about the data breach. That action was dismissed in Superior Court but reinstated by the Québec Court of Appeal.[19]

---

[17] Target can contest this amount, but has agreed not to appeal the trial court's determination so long as it does not exceed $20 million.

[18] *Zuckerman v. Target*, Judgment on Motion for Declinatory Exception and Subsidiarily for Forum Non Conveniens, No. 500-06-000686-143, 2015 QCCS 1285 (CanLII), Mar. 23, 2015 (J. Pinsonnault), *available at* http://canlii.ca/t/gh21w.

[19] *See Zuckerman v. Target*, Judgment, No. 500-09-025191-156, 2015 QCCA 1809 (CanLII), Nov. 6, 2015 (JJ. Bich, Savard, Schrager), *available at* http://canlii.ca/t/gm01p.

D. Congressional Committees

In the wake of the breach, congressional committees called hearings to investigate data security and sought information from Target. Representatives from Target were asked to appear at the hearings to testify about Target's data breach. Target's then CFO, John Mulligan, appeared before three congressional committees. At each of the hearings listed below, Mulligan provided written testimony to the respective committee, presented an opening statement, and testified:[20]

Date:	Committee:	Hearing Title:
February 4, 2014	Senate Committee on the Judiciary	"Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime"
February 5, 2014	House Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade	"Protecting Consumer Information: Can Data Breaches be Prevented?"
March 26, 2014	Senate Committee on Commerce, Science, & Transportation	"Protecting Personal Consumer Information from Cyber Attacks and Data Breaches"

Senators or representatives followed up with written questions to clarify the record. Target provided written responses to questions requiring follow up. Various reports were prepared for and as a result of these hearings.

In addition to Mr. Mulligan's testimony at these separate congressional hearings, Target provided information and requested documents to the House Committee on Oversight and Government Reform.

[20] Attached as Appendix D is the written testimony from each of the congressional hearings.

VI. The Special Litigation Committee

A. Establishment of the SLC

On June 11, 2014, in accordance with Minn. Stat. § 302A.241, Subd. 1, Target's Board of Directors established the SLC in response to the Demand. By resolution adopted on July 24, 2014, Target's Board expanded the SLC's charge to include all the derivative suits and any future actions that might be filed relating to the same subject matter. The Board appointed two non-Target-Board members, the Honorable Kathleen A. Blatz and Professor John H. Matheson, to the SLC and vested it with complete power and authority to investigate the allegations, claims, and requests for relief; to determine whether and/or to what extent Target should pursue those rights and remedies; and to respond to the litigation on behalf of the Board and the Company.

B. The SLC's Members

Neither member of the SLC had ever served on Target's Board of Directors, been employed by Target, or otherwise represented Target. As members of the Special Litigation Committee of the Board, they do not attend regular meetings and have no duties with respect to the operation of the business. The members of the SLC are solely tasked with executing the duties set forth in the resolutions, which are investigating the claims, determining the best interests of Target with respect to the Demand and derivative litigation, and responding on behalf of Target. Neither member has any material personal, professional, familial, or financial ties with Target or with any of the officers or directors named in the derivative actions or the Demand.[21]

[21] Target Corporation has two connections with the University of Minnesota Law School, which employs Professor Matheson. First, Target is one of 4,592 individuals or institutions that made financial donations to the Law School in 2015. Professor Matheson is not involved in the solicitation of donations to the Law School. Second, the University of Minnesota Law School's Corporate Institute places third-year law students in corporate externships. In 2015, 18

1. The Honorable Kathleen A. Blatz

The Honorable Kathleen A. Blatz was appointed Chief Justice of the Minnesota Supreme Court in 1998. She served in that capacity until her retirement on January 10, 2006. Prior to her appointment, she served as Associate Justice of the Minnesota Supreme Court and a Fourth Judicial District Judge, having been first appointed to the trial bench in 1994.

Chief Justice Blatz received a bachelor's degree from the University of Notre Dame, *summa cum laude*, Phi Beta Kappa. She received her Master of Social Work degree and her Juris Doctor degree, *cum laude*, from the University of Minnesota.

Prior to being appointed a judge, Chief Justice Blatz served in the Minnesota House of Representatives. In 1978, she was elected to the first of eight terms. During her legislative tenure, she served on various committees, including the Tax, Financial Institutions and Insurance, and Judiciary Committees. In addition, Chief Justice Blatz held several leadership positions, including that of Assistant Minority Leader and Chair of the Crime and Family Law Committee. During her legislative career, she practiced law at Popham, Haik, Schnobrich & Kaufman Ltd. and later as an Assistant Hennepin County Attorney.

Currently, Chief Justice Blatz is an attorney principally engaged as an arbitrator in commercial disputes. She is a qualified arbitrator for the American Arbitration Association and is on the roster of arbitrators selected for large, complex commercial disputes. She also serves on numerous boards, including as a director on the Columbia Funds Board, where she chairs the Governance Committee, and as a director/trustee on the Blue Cross Blue Shield of

---

organizations in the Twin Cities, including Target, participated in this program. Professor Matheson serves as Director of the Institute but does not participate in the placement of students for these unpaid corporate externships.

Minnesota/Aware Integrated, Inc. Board, where she chairs the Business Development Committee.

Throughout her career, Chief Justice Blatz has received numerous professional awards and recognitions, including being recognized as one of Minnesota Lawyer's Attorneys of the Year: 2011 Outstanding Service to the Profession and, in 2007, being recognized by Minnesota Law & Politics Legal Hall of Fame—100 Most Influential Attorneys in State History.

Chief Justice Blatz has also served on a special litigation committee for UnitedHealth Group, Inc. The special litigation committee was charged with investigating shareholder derivative claims involving, among other claims, breaches of fiduciary duties by its officers and directors.

2. ***Professor John H. Matheson***

John H. Matheson is the Law Alumni Distinguished Professor of Law and Director of the Corporate Institute at the University of Minnesota Law School. He is an internationally recognized expert in the area of corporate and business law and has taught in China, Germany, Ireland, England, the Netherlands, Uruguay, and Lithuania. He teaches courses in the business law area, including business associations/corporations, contracts, advanced corporate law, and comparative corporate governance.

Professor Matheson received a bachelor's degree from Illinois State University with high honors. He received his J.D., *cum laude*, from Northwestern University School of Law, where he was Editor-in-Chief of the Northwestern University Law Review. After completing his J.D., he clerked for Judge Robert A. Sprecher of the United States Court of Appeals for the Seventh Circuit. After his clerkship, Professor Matheson joined Hedlund, Hunter & Lynch (now Latham & Watkins) in Chicago. In 1982, he joined the University of Minnesota Law School faculty.

Professor Matheson is also a practicing lawyer. He is Of Counsel to Kaplan, Strangis and Kaplan, P.A., specializing in corporate governance counseling, fiduciary duties, mergers and acquisitions, and securities law matters. He is a member of the American Law Institute.

Professor Matheson's several books and numerous journal articles predominately address business and corporate law issues. He is in the process of publishing an article on derivative claims and special litigation committees. He recently published the third edition of his treatise on Minnesota Corporate Law, *Corporation Law and Practice*. One of Professor Matheson's co-authored articles, "Challenging Delaware's Desirability as a Haven for Incorporation," received the 2007 National Burton Award for Legal Excellence.

Professor Matheson also served as the reporter for the 2006, 2008, 2010, and 2014 amendments to the Minnesota Business Corporation Act. Although the Reporter's Notes do not have the effect of law, Minnesota courts often give them substantial consideration in statutory interpretation.

Professor Matheson has also served as the chair of a special litigation committee for Medtronic, Inc. That special litigation committee was tasked with investigating shareholder derivative claims involving, among other things, alleged director and officer breaches of fiduciary duties.

C. Retention of Counsel

In July 2014, the SLC retained Gaskins Bennett Birrell Schupp, LLP as its independent counsel to provide legal advice and to assist the SLC with all phases of its work, including document collection and review, planning and administration of the SLC's investigation, preparation for and participation in witness interviews, and selection and retention of various experts. Counsel has never represented Target or any of the individual defendants. Counsel

provided legal guidance concerning the available methods to resolve the claims against defendants in the derivative actions and putative defendants identified in the Demand and assisted in the preparation of the SLC's final report. The SLC has relied on the assistance and advice of its counsel throughout its investigation. Steve Gaskins and Sara Daggett have had primary responsibility for this undertaking.

Steve Gaskins received a bachelor's degree with special honors in 1970 and his J.D. with honors in 1973 from the University of Texas. He practiced law with Cleary, Gottlieb, Steen & Hamilton in New York from 1973 until 1979. He was an assistant district attorney in Manhattan from 1979 to 1982. In 1982, he moved to Minneapolis to practice law with Faegre & Benson and was a partner in the firm from 1984 to 1989. He has been a managing partner in his present firm since its inception in July 1989. Gaskins has maintained an active business and commercial trial practice and, in addition to serving as counsel to the Medtronic special litigation committee, has had significant experience with previous internal investigations and special litigation committees of publicly-traded companies. He is a Fellow of the American College of Trial Lawyers.

Sara Daggett received a bachelor's degree from the University of Wisconsin-Madison in 1997 and her J.D., *cum laude*, from William Mitchell College of Law in 2006. She joined Gaskins Bennett Birrell Schupp, LLP in 2008. She had an active commercial litigation practice until joining Minnesota's professional soccer club, Minnesota United FC, as its Vice President of Human Resources and Legal Affairs. Daggett previously served as counsel to the Medtronic special litigation committee.

Attorneys from Gaskins Bennett Birrell Schupp, LLP Robert Vaccaro, Ian Birrell, and Daniel Brees, as well as paralegal Allison Wittmer, also made material contributions to the SLC's investigation.

D. Experts

The SLC and its counsel conducted searches and retained two subject matter experts to analyze certain issues and relied on their expertise in the investigation.

1. Evan B. Francen, CISSP CISM

The SLC retained Evan Francen, co-founder and President of FRSecure LLC, a full-service information security company, to provide consulting services on the technical aspects of the data breach.[22] FRSecure LLC, among other services, performs PCI DSS assessments as a qualified security assessor. Francen is an information security expert with more than fifteen years of progressive technology and information systems security experience in both private and public companies. Among other certifications, he has held the Certified Information Systems Security Professional certification since February 2005 and the Certified Information Security Manager certification since June 2008.

Francen is well versed in governmental and industry-specific information security regulations, standards, and guidelines, including PCI DSS, HIPAA, GLBA, SOX, ISO 17799/27002 (information security), and COBIT. He is also knowledgeable about the intricacies in aligning security and compliance issues with business objectives. Francen has written in excess of 700 articles on information security and has developed and taught numerous information security courses. Other than being retained in this matter by the SLC, neither

[22] Mr. Francen's curriculum vitae is attached at Appendix E.

Francen nor his organization has performed services for Target or any of the individual defendants.

2. *William E. McCracken*

The SLC retained William McCracken to consult on issues of corporate governance related to data security.[23] McCracken graduated from Shippensburg University of Pennsylvania with a Bachelor of Arts in Physics. He worked at International Business Machines Corp. (IBM) for thirty-six years, from 1965 until he retired from IBM in August of 2001. He held various leadership roles at IBM including General Manager of IBM's PC Division overseeing Europe, the Middle East, and Africa (EMEA) from 1991 to 1993; Division President in the EMEA and Asia Pacific PC Division from 1993 to 1994; General Manager of the worldwide Marketing, Sales, and Distribution Division for the PC Division from 1994 to 1998; and General Manager of the Global PC Division from 1998 to 2001.

McCracken joined the Board of Directors of CA Technologies, a Fortune 500 software company that specializes in enterprise information technology management, on February 1, 2005 as an independent director. On that same date, as an independent director newly appointed to the Board, he was appointed to its special litigation committee to investigate various derivative actions revolving around CA's accounting practices and financial reporting systems. After the special litigation committee's investigation concluded, McCracken was appointed CEO of CA in January 2010 and served in that role until January 2013.

In 2009, McCracken was named by National Association of Corporate Directors (NACD) Directorship magazine as one of the top 100 most influential people in the boardroom; and, in 2010, he was named to the NACD Board. He was a commissioner of the NACD 2009 Blue

[23] Mr. McCracken's curriculum vitae is attached at Appendix F.

Ribbon Commission on Risk Governance and in 2012 was co-chair of the Blue Ribbon Commission on The Diverse Board. In 2015, he was co-chair of the Blue Ribbon Commission on The Board and Long-Term Value Creation and was a featured speaker at an NACD forum on cybersecurity. Other than being retained in this matter by the SLC, McCracken has never performed services for Target or any of the individual defendants.

VII. Overview of the SLC's Investigative Methodology

Over the past twenty-one months, the SLC has conducted an investigation into the circumstances surrounding Target's data breach. Its aim was to conduct its investigation in accordance with the fundamental principles of independence and good faith. During its investigation, the SLC has examined the roles of current and former officers, directors, employees, and third-party consultants in Target's data security program. In evaluating the claims detailed in the Demand and derivative complaints, it has focused on discovering reliable, truthful, and reasonably complete information about all the relevant issues and all aspects of the underlying claims; it considered the evidence it collected; it evaluated the credibility of the people it interviewed; and it deliberated on the many factors involved in determining what course of action would be in Target's best interests.

A. Documents

Throughout the course of its investigation, the SLC, with assistance from counsel, reviewed and analyzed thousands of documents, including electronically stored information. The documents can be categorized into five groups. First, throughout the investigation, the SLC propounded its own written information requests and document requests to Target, and Target fully cooperated, providing written answers and producing over 55,000 documents in response to those specific requests. Second, the SLC requested relevant documents from all of the director-

defendants. In response, they collectively produced approximately 1,300 documents. Third, the SLC had complete, unrestricted access to the database of approximately 465,000 documents produced in the Target MDL and maintained by Target's outside counsel. Fourth, the SLC requested and received the transcripts of all depositions taken in the Target MDL. Coordinating Lead Counsel over the MDL and Lead Counsel for the financial institution plaintiffs made deposition transcripts available to the SLC, as did counsel for Target. Finally, the SLC and counsel reviewed many documents available through public sources. Throughout its investigation, the SLC, in its role as a duly constituted Committee of the Board established to evaluate claims the company might have against its officers and directors, asked for and received from Target access to attorney-client privileged and other confidential information with the understanding that it would, absent intentional waiver, maintain its confidentiality.

At the SLC's request and under its supervision, counsel for the SLC performed comprehensive searches of all the available documents, reviewed and analyzed documents retrieved, reported on their findings, and provided thousands of pages of relevant materials for further review by the SLC. Document review and analysis by the SLC and its counsel continued throughout the investigation. During the course of its document review, the SLC and its counsel, with the help of its experts, analyzed and evaluated many different types of documents, including the following categories:

- documents produced to the Federal Trade Commission, the states' attorneys general, and the U.S. Securities and Exchange Commission during the course of those investigations;
- documents produced to the House Committee on Oversight and Government Reform relating to its inquiry;
- materials from pertinent congressional hearings, including John Mulligan's written testimony and transcript and recordings of congressional hearings at which he appeared;
- materials relating to the investigations of various government agencies;

- Target's Directors and Officers Liability policies;
- Target's network-security insurance policies for breach-related expenses;
- Target's contracts with the payment card networks;
- documents produced to and by the payment card networks during the card assessment processes;
- Target's full Board of Directors meeting minutes and materials from 2006–2015;
- Target's Audit Committee and Corporate Responsibility Committee meeting minutes and materials from 2006–2015, including successor committees;
- Target's Nominating and Governance Committee and Compensation Committee meeting minutes and materials from 2009–2014, including materials relating to the compensation of the directors, CEO, and other Executive Officers;
- Target's policies, procedures, and standards relating to the security and handling of customer information, privacy, incident response, and to the management of the Security Operations Center, which was responsible for monitoring and responding to possible network security threats;
- Target's training manuals and other training materials relating to information security and privacy;
- Target's pre-breach and post-breach organizational charts, as well as documents reflecting the headcount changes in information-security-related areas of Target;
- reports and relevant work papers from Target-engaged third parties, including Trustwave Holdings, Inc.,[24] Deloitte & Touche LLP,[25] The Chertoff Group, and Target's current PCI DSS assessor;
- Ernst & Young, LLP's ("Ernst & Young") annual integrated audit plan, quarterly review updates, updates provided to the Board, annual integrated audit results of the financial statements and internal control over financial reporting, as well as its opinions on the effectiveness of Target's internal control over financial reporting, its opinions on Target's consolidated financial statements, and its communications to the Audit Committee;
- industry standards and best practices, including the PCI Data Security Standard;
- documents reflecting Target's knowledge of and efforts to adhere to industry standards and best practices and its industry benchmarking activities;

---

[24] The PCI Council requires merchants to engage a third-party Qualified Security Assessor to assess the state of that merchants compliance with the PCI Standard as discussed *infra* at Part VIII.A. Target utilized Trustwave Holdings, Inc. as its pre-breach QSA company.

[25] The Chertoff Group and Deloitte & Touche LLP both conducted independent assessments of aspects of Target's information security program, discussed *infra* at Part IX.F.3.

- documents reflecting how Target collects and processes payment card data and Target's policies, procedures, practices, and activities related to that;
- technical documents such as network diagrams, internal and external penetration testing materials, documents related to Target's point-of-sale system, documents detailing the technical safeguards Target had in place designed to secure access to information on Target's systems, and documents detailing particular vulnerabilities exploited by the hacker;
- Target's internal audit, compliance, and enterprise risk management materials pertaining to technology and information security;
- procedures governing assessment of technical risks and documents reflecting the evaluation of specific technical risks;
- human resources documents, including relevant separation agreements of former Target officers and documents relating to those agreements, as well as HR files and compensation information of key employees, including officer-defendants and other employees with significant roles in information security;
- financial documents, including documents reflecting Target's general financial status, as well as documents reflecting information-security-related budgets and funding, direct and indirect expenses relating to the data breach, and accelerated investments as a result of the breach;
- documents relating to Target's information security committees, task forces, and other working groups;
- internal and external forensic reports setting forth the technical facts of the data breach;
- documents relating to Target personnel's handling of the security alerts during the breach;
- documents reflecting the response of the officers, directors, and information security employees after discovery of the breach, including internal communications;
- documents relating to public communications and customer notifications regarding the breach, as well as customer reactions;
- documents relating to post-breach remediation activities, governance changes, and additional technical safeguards put in place;
- public information relating to data security risks, other data breaches, and the evolution of the risk landscape;
- documents relating to other retailers' security and risk oversight practices and public disclosures;

- documents detailing the 2007 attack on Target's computer networks referenced in the consolidated complaint and Target's response to that attack; and
- documents reflecting Target's security-related vendor assessment practices and vendor contracts.

The SLC and its counsel also accessed and analyzed Target's financial reports and disclosures through the SEC's EDGAR database, including Target's form 10-Ks, form 10-Qs, its annual definitive proxy statements along with definitive additional materials when available, and various 8-Ks during the relevant period. The SLC and its counsel also accessed and analyzed pleadings, decisions, and other papers in the related cases and investigations, including legal holds issued to Target employees and directors. Counsel accessed, read, and analyzed various information-security-related articles and articles concerning corporate-risk governance, including information-security-risk governance in particular, and discussed these topics with the SLC and its experts. The SLC members themselves conducted research on pertinent topics, such as the corporate governance of information security risk.

B. Interviews

The SLC, with counsel, conducted 73 interviews of 68 individuals[26] (five individuals were interviewed twice).[27] These interviews were a key part of the SLC's investigative process as they helped the SLC corroborate and contextualize the documentary information it had gathered, evaluate the significance of data, gain an understanding of Target's corporate culture—especially as it related to data security—assess employees' morale, understand employees' attitudes towards Target's data security policies and processes, and determine how those policies and procedures were implemented throughout the company. The SLC members actively

[26] Two former Target employees declined to be interviewed, Milinda Rambel Stone, who declined through counsel, and Kurt Lieber.

[27] A full list of the interviews conducted during the investigation is attached as Appendix G.

participated in all these interviews. Most of the interviews were conducted in-person, with the exception of three that were conducted via videoconference. The SLC members traveled to Washington, D.C. twice, New York City, and San Diego[28] to conduct interviews during the course of its investigation.

Those interviewed included:

- all the named defendants, including Target's current and former officers and current and former members of Target's Board of Directors;
- personnel from Target's general counsel's office;
- current and former members of Target's corporate security team, including employees involved in business continuity, physical security, internal forensic investigations, and cyber intelligence;
- members of the Target Information Protection (TIP) team, including employees involved in the following: compliance, audit support, security project management, development of information security policies and procedures, incident response, cybersecurity, vendor assessments, Target's Intake Team, internal security training and awareness, risk assessment and response, the management of data loss prevention tools, and privacy;
- members of the Target Technology Services (TTS) team, including its dedicated security team and employees responsible for the following: responding to security alerts, server technology development, remote access services, penetration testing, system architecture, access provisioning, infrastructure planning, and software technology assessment and development;
- members of Target's engineering team, located within TTS, which built, assessed, and ran various component parts of Target's computer network;
- members of Target's point-of-sale hardware engineering team, located within TTS, who maintained the point-of-sale systems, including payment terminals and peripherals;
- members of Target's network engineering team, located within TTS, who worked on security engineering, were involved on the implementation side of network design and segmentation, and who were familiar with network monitoring tools;
- members of Target's internal audit team, including employees involved in auditing data security processes and controls;
- Target employees who assisted in post-breach remediation;

[28] One SLC member traveled to San Diego; the other participated via conference call.

- members of Target's team that oversaw security technologies and determined what security tools Target should implement;
- leaders of Target's new Cyber Fusion Center;
- a consulting expert retained by Target's outside counsel, Morrison & Foerster;
- the lead PCI Forensic Investigator hired in Target's post-breach investigation;
- the lead assessor in 2012 and 2013 responsible for the assessment of Target's compliance with the Payment Card Industry Data Security Standard (PCI DSS);
- the Senior Vice President of Enterprise Risk Management and Information Security for Target's pre-breach Qualified Security Assessor company; and
- the lead audit partner for the Target engagement from Ernst & Young, Target's independent auditor.

In addition to the 73 interviews in which the SLC members participated personally, as part of the investigation, counsel conducted two supplemental interviews and reported to the members of the SLC the substance of the interviews, issues raised, and information gleaned from the interviews. These interviews were of employees involved in risk assessments and risk treatment. Counsel also met and had telephone conversations with a number of attorneys possessing relevant information, including Coordinating Lead Counsel in the MDL.

C. SLC Meetings

Throughout its investigation, members of the SLC and counsel, in addition to engaging in telephone calls on a regular basis, met in person on more than 100 occasions. The SLC reviewed the evidence developed, analyzed legal memoranda provided by counsel, assessed the credibility of the witnesses, and ascertained what additional information might be necessary or desirable in order to determine what course of action would be in the best interests of Target.

During one meeting, the SLC toured Target's new Cyber Fusion Center and met with Brad Maiorino, Target's Chief Information Security Officer, Dave Baumgartner, Target's Vice President of Cyber Security, Rich Agostino, Vice President of Information Security, and Tim

Crothers, Senior Director of Cyber Security, to discuss Target's cybersecurity teams and their roles. While the on-site visit to the Cyber Fusion Center was not considered a formal interview, the SLC members and counsel asked questions of the Target employees present.

At another meeting, and at the SLC's invitation, Target's counsel gave a presentation on the facts and issues raised in the Demand and derivative complaints from Target's perspective.

Wilmer Cutler Pickering Hale and Dorr LLP, counsel for the individual director defendants, requested the opportunity to make a presentation on behalf of its clients. The SLC agreed to hear the presentation during part of one of its meetings.

The SLC also twice—at the beginning and toward the end of its investigation—invited counsel for the derivative shareholder plaintiffs and Demand shareholder to make a presentation on the issues arising from their allegations, including their view of the factors bearing on whether there were rights and remedies Target had against the defendants named in the complaint that were in Target's best interests to pursue. Counsel for the consolidated federal derivative plaintiffs, along with the counsel for the state derivative plaintiff, responded with a telephone presentation and a written submission in October 2014. They also provided a written submission in response to the SLC's second invitation in February 2016.

The SLC, in conducting its independent investigation, considered and evaluated the derivative plaintiffs' counsel's investigative suggestions, including suggested interview questions, witnesses, and experts. While the SLC considered the perspective offered by plaintiffs' counsel, it conducted its own investigation and did so independently. It did not share the information it gathered or its conclusions with the plaintiffs, the individual defendants, Target, or their respective counsel before it issued this report.

D. Analysis and Deliberations

The SLC was mindful that it would ultimately have to decide whether Target should accept or reject, in whole or in part, the Demand's call for legal and other remedial action, whether it should start its own legal action, or whether it should seek other remedies. It was also mindful that it would have to decide whether Target should intervene in—and take over the prosecution of—the derivative actions, seek dismissals, or simply abstain and allow the plaintiff shareholders to proceed derivatively on Target's behalf.

Through its investigation, the SLC was able to gather information about Target's information security program and the data breach, assess the factual and legal claims made in the Demand and derivative cases, and determine what course of action is in the best interests of Target to pursue. The SLC's evaluation and assessment included the following:

- the SLC considered the history of developing cybersecurity threats, data breaches, and point-of-sale malware in the months and years before the data breach, as well as the extent of Target employees', officers', and directors' knowledge of general and specific cybersecurity threats;
- the SLC analyzed details of the 2007 attack on Target's computer networks, including Target's response to that attack and the similarities and differences between that attack and the data breach;
- the SLC considered the strengths and weaknesses of Target's pre-breach data-security-related policies and procedures;
- the SLC evaluated Target's pre-breach and post-breach corporate governance structure as it related to data security;
- the SLC considered and investigated the claim that Target's management ignored concerns raised by its information security employees about vulnerabilities in Target's payment card system prior to the data breach;
- the SLC assessed customer notifications after the breach, including the information Target provided regarding debit card PIN data and whether the information was accurate and reasonably timely in light of the facts as they were being discovered;
- the SLC gathered and assessed the correspondence and the information Target provided and received in various post-breach investigations of Target's practices, including those conducted by the SEC, FTC, and states' attorneys general;

- the SLC evaluated Target's PCI compliance both pre-breach and post-breach;
- the SLC considered information about relevant alerts fired during the data breach and evaluated the decisions made by the employees handling them;
- the SLC evaluated Target's data security systems and technologies, including vulnerabilities exploited by the hacker during the breach, the measures Target took to address vulnerabilities in its system before the breach, and the remedial measures Target took after the breach;
- the SLC considered whether there were red flags prior to the breach and, if so, whether they were appropriately responded to and by whom;
- the SLC considered pre-breach and post-breach audits of Target's internal controls over financial reporting, including assessments of information technology general controls relating to security;
- the SLC considered Gregg Steinhafel's compensation and separation agreement and evaluated the business reasons provided by the Board for entering into that agreement;
- the SLC assessed whether Target followed industry best practices with respect to data security in general and payment card security in particular;
- the SLC evaluated the pre-breach and post-breach competency of Target's employees, including the named defendants and Target's employees responsible for data security, and the credibility of those interviewed;
- the SLC evaluated Target's pre-breach and post-breach risk assessment and risk management policies and practices;
- the SLC considered whether people were employed in appropriate positions for their skill level and background;
- the SLC assessed Target's remediation efforts post-breach, including changes made to Target's corporate governance structure for its information security program;
- the SLC evaluated Target's pre-breach vendor security procedures and the remediation efforts after the breach;
- the SLC evaluated Target's investments in network security personnel, processes, and technologies between 2007 and 2013, as well as Target's investments in these after the breach;
- the SLC evaluated information on the number of Target employees dedicated to information security between 2007 and 2013;
- the SLC considered the overall financial impact of the breach, including litigation expenses and settlements, cost of fraudulent transactions, credit monitoring expenses, call center expenses, the level of customer traffic, cost of promotions offered to increase

traffic, potential increased cost of capital due to debt rating downgrades, card reissuance expenses, and costs associated with a slowdown in REDcard applications;

- the SLC considered the short- and long-term fluctuations in stock price after the breach;
- the SLC evaluated Target's employee data security training; and
- the SLC evaluated the types of network monitoring software Target had in place pre-breach and assessed whether they were reasonable.

The SLC is confident that it has received sufficient pertinent information to understand the facts and the relevant parties' positions and views and to reach an informed, reasoned judgment as to the best interests of Target with respect to the derivative actions and the shareholder Demand.

VIII. Regulation of Information Security

Many companies, including retailers, store and process sensitive information about customers and employees on their computer networks. Protecting the security and privacy of such information has become an increasingly public concern. As a result, industry self-regulators and state and federal government agencies have required companies to meet certain substantive data security requirements. A complex network of laws, regulations, and industry agreements have developed and are continuing to develop around these issues.

A. The Payment Card Industry Data Security Standard (PCI DSS)

In order to mitigate the risk of fraud, the major card brands developed contractual rules about necessary security measures that merchants and other entities were required to follow in order to process the brands' payment cards. In 2004, five of the major card brands[29] established version 1.0 of a singular, unified standard called the Payment Card Industry Data Security Standard (PCI DSS). In 2006, these five card companies established a formal Payment Card

[29] American Express, Discover, JCB, MasterCard, and Visa.

Industry Security Standards Council that had the purpose of managing the ongoing evolution of the PCI DSS.

The PCI process is a way for merchants and banks to allocate the risk of loss in the event of a breach. It also seeks to minimize the likelihood of breaches by instituting substantive requirements for merchants who accept payment cards.

Under the provisions of interrelated contracts among payment card issuers, card brands, card processors, and merchants, merchants are required to adhere to the PCI DSS as a condition to accept payment cards. If merchants are noncompliant, they may face penalties as dictated by these contracts, including fines, the inability to accept cards, and potentially increased liability in the event of a breach. Merchants are required to validate their compliance annually. For companies handling a large number of payment card transactions, like Target, PCI DSS requires independent validation through an annual assessment by an external Qualified Security Assessor who examines the merchant's payment card security system and provides a Report on Compliance.

Version 2.0 of the PCI DSS was in effect at the time of the data breach. Under version 2.0, PCI DSS had 12 main requirements and 211 sub-requirements that merchants were required to follow. Taken together, the requirements spanned a number of interconnected fields, including encryption, network monitoring and testing, access controls, vulnerability management, and maintenance of an information security policy.

B. State and Federal Regulation of Information Security

In addition to this industry-created standard, organizations must comply with federal and state standards relating to information security arising from several different statutes and

associated rules and regulations, which are enforced by various state and federal agencies. The federal statutes include:

- the Gramm-Leach-Bliley Act (GLBA),[30] which regulates the operations of financial institutions, including how they notify customers about information-sharing practices and how they secure customer information. GLBA is enforced by different agencies depending upon the nature of the financial institution at issue, including federal banking agencies, the board of the National Credit Union Administration, the SEC, various states' insurance authorities, and the FTC;

- the Sarbanes-Oxley Act of 2002 (SOX),[31] which attempts to protect shareholders and the public at large by minimizing accounting errors and fraud by improving the accuracy of financial disclosures. SOX is enforced by the SEC and the Public Company Accounting Oversight Board;

- the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[32] which establishes substantive data protection requirements regarding the protection of sensitive health information. HIPAA is primarily enforced by the U.S. Department of Health and Human Services Office for Civil Rights;

- the Health Insurance Technology for Economic and Clinical Health Act (HITECH),[33] which modified HIPAA by increasing the rigor of enforcement and the monetary fines associated with non-compliance. HITECH has a number of components, including expansion of the notification requirements for data breaches of personal health information;

- the Children's Online Privacy Protection Act of 1998 (COPPA),[34] which regulates companies' and individuals' online collection of personal information from children under 13 years of age. COPPA is enforced by the FTC and other state and federal agencies based on the field and industry being regulated;

- the Fair Credit Reporting Act (FCRA),[35] which regulates the collection, dissemination, and use of consumer credit information, particularly as it relates to credit reports. The FCRA is enforced by the FTC and the Consumer Financial Protection Bureau; and

---

[30] The Gramm-Leach-Bliley Act was also known as the Financial Modernization Act of 1999. GLBA is codified in relevant part at 15 U.S.C. §§ 6801–6809 and §§ 6821–6827.

[31] Pub. L. No. 107-204 (codified throughout parts of Titles 15, 18, and 28 of the United States Code).

[32] Pub. L. No. 104-191 (codified throughout parts of Titles 26, 29, and 42 of the United States Code).

[33] HITECH is part of the American Recovery and Reinvestment Act of 2009. Pub. L. No. 111-5 (codified throughout parts of Title 42 of the United States Code).

[34] 15 U.S.C. §§ 6501–6506.

[35] 15 U.S.C. § 1681.

- the Fair and Accurate Credit Transactions Act of 2003 (FACTA),[36] which amended the FCRA.

In addition to the enforcement authority noted above, the FTC also has the power to regulate unfair or deceptive acts or practices (UDAP) pursuant to the Federal Trade Commission Act of 1914.[37] A company's actions can be deemed deceptive if the company materially misrepresents the state of its data security program to consumers. Separately, a company's acts may be deemed unfair if the company's acts or practices unjustifiably cause consumer injury. As the Commission put forth in a "Statement Marking the FTC's 50th Data Security Settlement":

> The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. Through its settlements, testimony, and public statements, the Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.[38]

To execute its mandates, the FTC has the authority to bring enforcement actions against companies. That authority, as applied to actions involving cybersecurity, was recently upheld in *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015). FTC commissioners have also publicly noted that even if a company were deemed PCI compliant, that would not necessarily be sufficient to establish the existence of reasonable and appropriate security measures within that company, although the FTC does take that into consideration as a factor in evaluating the reasonableness of a company's security practices.

---

[36] Pub. L. No. 108-159 (amending 15 U.S.C. §§ 1601–67, 1681).

[37] 15 U.S.C. §§ 41–58.

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

The SEC also regulates cybersecurity and, on October 13, 2011, issued guidance on companies' cybersecurity disclosures. The Commission's two main investigative focuses are: (1) the adequacy of companies' financial disclosures of cyber risks and events and (2) the internal controls, policies, and procedures companies maintain to mitigate cyber risk.

Additionally, nearly all states have instituted laws governing companies' information security protocols, including laws governing (1) substantive data protection requirements, (2) how companies must notify the public after a breach, and (3) whether a lack of controls resulting in a data breach can constitute an unfair or deceptive act barred under state law.

IX. Target's Pre-Breach Information Security Program

In 2008, Target issued its first written Information Protection Program Charter, which established the high-level goals of Target's broad information security program. The Charter was revised on occasion, and the version in place at the time of the breach was signed by Target's general counsel, its CIO, and the head of its Financial and Retail Services (FRS) division. Target's information security program at the time of the breach is described below.

A. Administrative Structure of Target's Information Security Program

Although many of Target's teams played at least some role in protecting customer information at the time of the data breach, three teams had the primary, interrelated responsibility for protecting personal data: Target Information Protection (TIP); Target Technology Services (TTS); and Corporate Security. TIP and TTS were designed to collaborate on a day-to-day basis by sharing information and addressing related issues.

1. Target Information Protection (TIP)

In late 2007, Target's Executive Committee approved the initial formation of TIP. TIP's mission was to "[s]afeguard Target's reputation by providing a sustainable, enterprise-wide

information security and privacy program that engages team members, informs business risk decisions and protects guest, team member and company information." TIP's role in information security included: (1) establishing Target's information security policies and standards; (2) implementing and administering the security policies and standards; (3) working with third-party assessors and various Target teams to manage Target's compliance with external standards; (4) managing Target's response to non-routine network security incidents; (5) engaging other Target teams to understand Target's business needs and, when appropriate, incorporating those needs into Target's security practices; (6) prioritizing information-security-related investments and programs; and (7) developing a proactive, rather than a reactive, approach to security across Target. TIP also coordinated knowledge and brought in expertise from other Target business units. TIP based its actions and documentation on the standards provided by the International Organization for Standardization, commonly referred to as ISO.

From 2010 until the time of the data breach, TIP was led by a senior director-level manager, whose internal duties included responsibility for numerous aspects of data security and compliance as well as the roles of Chief Privacy Officer and HIPAA Security/Privacy Officer. At the time of the breach, the senior director in charge of TIP reported to the President of FRS, who reported to the CFO.

TIP contained specific teams that managed areas such as vendor security, privacy, information risk management, records retention, and training and awareness related to Target's security policies. Notable teams included:

a. Vendor Assessment and Management Team

Target had policies, procedures, and standards in place governing vendor access and security. Vendors, by contract, were required to meet Target's security standards. Target's

policies required vendors to complete a risk profile that determined the level of inherent risk a vendor posed based on a number of factors, including the class of data being used and the vendor's connectivity to Target's network. The risk profile was a series of questions encompassing the vendor's services, IT risk management, and data security practices.

Target had a dedicated Vendor Assessment and Management Team housed within TIP to determine whether vendors should be able to access Target's network and to perform assessments on vendors based on the vendor's risk. Not all vendors were independently assessed, and whether they were assessed or not was principally dependent on the inherent risk assessment score. The team conducted approximately 300 vendor assessments each year.

b. Risk Review Committee

TIP also led Target's cross-functional Risk Review Committee (RRC). The RRC was founded in 2010 with the stated mission "to protect team members, guests, and Target by engaging business partners to reduce risks through the use of a repeatable Information Risk Management framework that identifies risks, defines priorities, and provides security options to treat those risks." The majority of the RRC's members were from TTS and TIP, but individuals from Target's legal team and various business teams also participated.

When business teams and technology teams identified a security issue and needed guidance, they requested guidance from the RRC. The RRC then determined whether the risks were acceptable or whether additional risk mitigation was necessary. The RRC received information on potential risks from a variety of sources, including compliance assessments, enterprise risk assessments, incident investigations, vulnerability scans, virus scans, and audit findings. The RRC did not itself manage the mitigation of risks, but provided guidance to the business and technology teams as needed. In addition to considering and providing guidance on

individual risks before it, the RRC aggregated high-level themes surrounding the risks presented to it and reported to the Cyber Executive Committee about these risks. The Cyber Executive Committee is discussed below.

c. Intake Team

In 2011, TIP created an Intake Team to provide an avenue for Target employees to address general security-related questions or concerns. For example, if an employee lost a laptop, received a suspicious email, or had a security question relating to a project, the Intake Team provided a ready resource for employees to bring their issues to TIP's attention. The Intake Team did not itself resolve complex issues but rather answered common questions and directed the more complicated issues or questions to an individual or team with sufficient technical expertise to address them.

2. Target Technology Services (TTS)

TTS was Target's broad-based information technology team and was led by Target's CIO. The CIO reported directly to the CEO. Its general role was to plan, build, and run Target's computer systems. TTS's responsibilities extended across Target's entire technology portfolio and included managing the corporate network, Target's corporate data centers, each of the store networks, the point-of-sale registers contained in the store networks, and Target.com. At the time of the breach, a number of teams worked within the TTS organization: Target.com, Technology Strategy and Enterprise Architecture, Mobile and Marketing, Solution Delivery and Engineering, and Infrastructure and Security, among others. Target's information technology teams in India and Canada were also part of the TTS organization. Including employees and contractors in the United States and abroad, in late 2013, TTS employed roughly 9,000 workers.

TTS had a standing cybersecurity team that reported to the CIO through both a senior director and a vice president. That team was responsible for implementing new technology security capabilities and maintaining existing capabilities. The TTS security team was subdivided into areas of focus, including management of access rights; data protections tools, processes, and controls; security issues arising during application development and application onboarding; monitoring and logging data at rest and in transit; and identifying, investigating, and eliminating exploitable technological risks.

Other teams within TTS, such as the Enterprise Architecture team, were not specifically dedicated to information security but were assigned work with security implications. These teams worked with other Target teams to identify best practices relating to security and ways in which Target could structure its operations to be most effective. TTS's other notable teams with major security roles included the SOC and Target's Red team, which are discussed below.

a. Security Operations Center (SOC)

Target's SOC, created in 2008, was Target's around-the-clock alert management center. The SOC monitored Target's network for anomalous activity, determined whether activities posed security concerns, and worked with TIP to address the identified security concerns. In doing so, the SOC operated under a defined set of written policies specific to its operations.

At the time of the breach, Target's automated systems logged approximately 850 million computer occurrences per day, such as a user logging into an account, sending an email, or opening a file. Target's automated systems triggered "alerts" on occurrences if they met certain pre-defined conditions. Target's systems triggered approximately 200 alerts per day. All alerts were analyzed by humans within a defined system of analysis and escalation.

If an analyst determined that an alert was serious enough—due to a significant probability of compromising employee information, customer personal information, or confidential business information—the alert was escalated to TIP, which coordinated its resolution with support from the SOC, the involved business unit, and/or the Information Security Investigations team (ISI).

b. Red Team

In 2012, TTS established its Red team. A "red team" is an industry term for an internal security team comprised of ethical, "white-hat" hackers. Target's Red team conducted its own network security tests, which were designed to find security vulnerabilities and assess Target employees' responses to their probes. The Red team operated by simulating both covert and overt attacks on Target-owned systems and resources and then assessing the adequacy of Target's efforts to detect the attack and take appropriate action. The Red team reported vulnerabilities to the appropriate teams and cooperated with them to remediate revealed vulnerabilities. The Red team's probes were both technical and non-technical in nature.

3. Corporate Security and Information Security Investigations (ISI)

Target's Corporate Security department housed the investigative arm of Target's data security program and its cyberintelligence team. At the time of the breach, it was headed by the Vice President of Corporate Security, who reported to the general counsel. ISI forensic analysts helped investigate incidents in coordination with the SOC and TIP. The cyberintelligence team was organized to identify known and developing intelligence and data security risks and to report on notable findings to business units that would benefit from the knowledge.

B. Cybersecurity Program Governance

Target's cybersecurity program architecture was organized primarily in three levels. Target's Cyber Executive Committee, which met quarterly, oversaw this program. The Cyber Executive Committee consisted of senior representatives from Corporate Security, FRS, and TTS.

Reporting to the Cyber Executive Committee was the Cyber Steering Committee. The purpose of this group was to bring the individual teams together to plan for the future of Target's cybersecurity program. In addition, the Cyber Steering Committee reviewed the cybersecurity program strategy and progress, made key decisions on cybersecurity initiatives, negotiated priorities between the Cyber Executive Committee and the Cyber Working Group, and prepared agendas for the Cyber Executive Committee meetings. Leaders from TIP, TTS, and Corporate Security made up this committee. The Corporate Security team provided cyber-related information and intelligence to the Cyber Steering Committee.

A Cyber Working Group gathered information from internal and external sources, discussed what was happening in the cyber realm, and reported to the Cyber Steering Committee on threat and vulnerability trends. The working group's members included representatives from TIP, TTS, and Corporate Security.

C. Policies and Procedures

Before the breach, Target had enacted policies, procedures, and standards for protecting systems that collect, process, transfer, and store personal information. The policies governed a broad array of areas, including SOC management, access management, asset management, network scanning, risk review practices, and other areas relating to information security. Target

also developed an incident response plan addressing how Target should handle certain types of security incidents.

Target's information security governance was shaped by its three fundamental documents: the Target Information Protection Program Charter, the Target Information Protection Policy, and the Target Information Protection Standard. Target adopted initial versions of these in 2008, 2011, and 2012, respectively, and updated them regularly. The specific versions discussed in this section are those that were in place at the time of the breach.

1. Target Information Protection Program Charter

Target's Information Protection Program Charter (the "Charter") governed Target's operations as applied to information protection, including information security, privacy, and records management. TIP managed the Charter, which applied to all of Target's business units as well as to anyone with access to Target information assets, including all employees, contractors, and vendors. The Charter emphasized that "Target executive management is committed to safeguarding Target information assets" and directed the establishment and management of a Target-wide data protection program. The Charter also set forth Target's "Information Protection Mission," which was to "provide Target Corporation with a sustainable, enterprise-wide information protection [program] that engages team members, informs business risk decisions, and protects guest, team member, and company information."

The Charter also established executive oversight committees. Those committees provided oversight for Target's data protection program, received information from Target business units, and directed business involvement. The Charter set forth Target's goal to make "information protection a core competency at Target" and established three general principles to

strive to meet that goal: (1) making information protection part of Target's culture; (2) supporting Target's business priorities; and (3) standardizing Target's practices.

2. *Target Information Protection Policy*

Target's Information Protection Policy (the "Policy") was managed by TIP and established a minimum baseline for how employees protected information and ensured privacy of sensitive information. The Policy required employees to ensure the security and confidentiality of Target information, including customer information. The Policy referenced Target's Information Classification and Handling Standard, which was adopted in 2007 and updated regularly. Information was divided into four classifications, each with different handling requirements: public, internal, confidential, and secure handling required. The Policy also proscribed certain specific conduct, such as directly connecting unauthorized hardware to the network, attempting to circumvent or modify configurations or access controls, downloading or using unauthorized software, opening suspicious attachments, and using insecure passwords. The Policy noted that violation of the security requirements it outlined was grounds for disciplinary action, including potential termination and legal action. The Policy urged compliance and provided an anonymous hotline for employees to call to report instances of non-compliance.

3. *Target Information Protection Standard*

TIP created the Target Information Protection Standard (the "Standard"), a specific standard based on the Policy. The Standard applied to all Target information assets and resources. The 71-page Standard established protocols, requirements, and sub-requirements across 28 subjects. The subjects included the following: access control and identity management; application security; change management; customer financial privacy; encryption;

event and incident response; information risk management; network control; passwords; policy management; records management; system monitoring; training, awareness, and education; and vendor engagement.

As to each area, the Standard articulated requirements for information handling and network security. Like the Policy, the Standard also identified which teams within Target were responsible for implementing the Standard's requirements.

The Standard established that Target employees were responsible for complying with its requirements and repeated that violating those requirements could result in disciplinary action, up to and including termination and legal action. The Standard also identified the anonymous hotline for reporting non-compliance.

4. Information Classification and Handling Job Aids

Target also developed job aids—procedures specific to given business areas. TIP published the job aids and distributed them to more than a dozen individual divisions in Target. Each job aid explained what the four information classifications were (public, internal, confidential, and secure handling required) and explained how employees in each individual division should classify various types of information with which they interacted on a day-to-day basis. They also explained how employees were required to treat data under each classification and provided explicit procedures for employees to follow.

5. Training

Target trained its employees on the existence and content of its data security requirements through an annual formal training program called "Protecting Information at Target" (PIAT). A team within TIP managed the training, which it conducted primarily through computer programs. Employees were required to take a test after they received the training, and

TIP analyzed the results to determine how effective the training was at conveying Target's requirements. The training generally covered information protection expectations, policies, best courses of action with respect to data protection generally, and reporting instructions regarding information protection issues.

Employees received additional training depending upon their job focus; for example, employees who handled payment card information received PCI DSS compliance training to supplement the PIAT training. Employees working in stores received alternative security training from supervisors and managers at those stores. Target employees were also trained on the risks related to phishing and were told to report suspicious emails or potential concerns to TIP's Intake Team. Employees were also subject to simulated phishing attacks by TIP personnel.

Additionally, TIP facilitated Target Information Protection month, during which printed materials about Target's security practices were made available to employees at Target stores and in common areas at Target headquarters.

D. Technical Safeguards in Place

At the time of the data breach, Target had established certain technical measures aimed at protecting the security of Target's network and the information in it. These measures included:

- various methods of managing user network access, such as account passwords, firewalls, switches, proxy servers, and routers with access control lists;
- intrusion detection and prevention tools;
- security incident and event monitoring tools utilized by the SOC;
- data loss prevention tools;
- network scanning tools;
- web filtering and proxy management tools;
- antivirus software;

- restrictions on wireless network access;
- data encryption;
- advanced threat detection software; and
- file integrity monitoring.

Target also conducted a number of tests and scans to verify the integrity of its technical systems, such as vulnerability scanning, penetration testing, and application security testing, discussed below.

1. Vulnerability Scanning

Target's infrastructure security team located within TTS performed both internal and external vulnerability scanning with the aim of identifying potential gaps in Target's network, such as the use of unsupported or out-of-date software. Target used a commercial vulnerability-scanning tool to facilitate this process.

2. Penetration Testing

Penetration tests are computer probes designed to test the strength and capability of portions of a computer network. These tests focused on defined segments of Target's network and followed a structured process to determine whether the area of the network being tested was vulnerable. Penetration tests, which are required by PCI DSS to test the integrity of the cardholder data systems, fall into two categories—internal penetration testing and external penetration testing. Internal penetration testing is launched from inside a network with the aim of moving to other restricted areas within the network. External penetration testing is launched from outside a network with the aim of getting into parts of the network by bypassing firewalls that were designed to deny outside access. Target and third parties conducted internal and external penetration tests on various portions of Target's network, including those that processed cardholder data.

3. *Application Security Testing*

Target tested applications[39] for vulnerabilities using various combinations of techniques, including static code scanning, dynamic code scanning, and application penetration testing. Where the tests revealed a vulnerability, Target remediated it on an as-needed basis. Target also established baseline information security requirements for applications developed in-house or by third parties.

E. Physical Safeguards in Place

Target had protocols in place to limit physical access to and tampering with hardware, including Target's corporate servers, store servers, and its point-of-sale registers. Target's physical security policies were set forth in the Standard and adherence to the policies was monitored by internal and external audits, including visual inspections. Target's controls included security guards, access badging, and live video monitoring. Additionally, Target policy only allowed individuals to physically access computer networks and systems upon a showing of business need and provided greater protection for sensitive areas, such as data centers.

F. Internal and External Validation of Safeguards

At and before the time of the breach, Target used multiple formal mechanisms to attempt to validate the existence and efficacy of the policies and safeguards it had in place. In addition to the formal validation structures and processes described below, some validation was done through informal processes, such as status updates with supervisors and ad-hoc discussions when issues arose.

[39] An application is a computer program designed to perform either a single discrete task or a group of such tasks. Microsoft Word and Internet Explorer are examples of applications.

1. Internal and External Auditors

Target had a department called Assurance, Risk, and Compliance (ARC) that reported to the CFO and to the Board's Audit Committee. Assurance, a branch of that department, served as Target's internal audit function. Assurance assessed Target's policies, procedures, and practices, and compliance with them.

Target Assurance employees were required to comply with the International Standards for the Professional Practice of Internal Auditing. Assurance prepared an annual audit plan that the Audit Committee reviewed and approved at the beginning of each fiscal year. The audit plan was informed by a continuous risk assessment performed by Assurance, Target's strategic initiatives, enterprise risk reviews, compliance work, and prior-year audits.

Target Assurance performed six types of engagements: audits, SOX, assessments, consultations, projects, and follow-ups from previous findings. Assurance had multiple teams, one of which was Target Technology Assurance. This team was responsible for auditing the effectiveness of controls for Target's support functions, including information technology, human resources, and financial and retail services. TTS Assurance, a group within Target Technology Assurance, was responsible for assessing technological risks and auditing the information technology function, with a focus on system and application security. TTS Assurance audits were planned using a risk-based approach, and by 2009 and every year thereafter, information security was considered a significant enterprise risk.

Ernst & Young served as Target's independent external auditor. As part of its annual audit, it evaluated Target's Assurance employees' skillsets, independence and objectivity, and competence to determine to what extent it could rely on Assurance's work. Target Assurance

provided Ernst & Young with every internal audit report it generated, and Ernst & Young used the reports, in part, to design its own independent audit plan.

Each year, Ernst & Young's information services team tested and audited the information technology general controls (ITGC), which included three primary areas of focus: logical access, change management, and IT operations. Each of these areas have security implications. In the testing of ITGC, and more specifically security-related ITGC, prior to the breach, Ernst & Young found no significant deficiencies or material weaknesses in Target's internal controls. Ernst & Young reported its audit findings to Target management and the Audit Committee of Target's Board of Directors.

2. Compliance

Target's compliance and ethics program's published objectives were to promote an organizational culture that encouraged ethical conduct and a commitment to legal compliance. All employees were expected to exercise due diligence to prevent and detect compliance-related criminal conduct. The Board and Audit Committee oversaw the implementation of and effectiveness of the compliance program. That oversight was accomplished through reports from management to the Audit Committee and through updates by the Audit Committee to the full Board. Management's Executive Committee (comprised of executive-level management) acted as the Corporate Compliance Committee; and the Vice President of Assurance, Risk, and Compliance served as the Chief Compliance Officer and, as CCO, reported directly to the Audit Committee and to management's Executive Committee. The Audit Committee reviewed the Compliance Charter annually.

Under the Compliance Charter, business teams within the Company were accountable for compliance within their respective business units. As a result, most of the compliance policies

were associated with specific parts of the business. Data security policies were drafted and owned by TIP.

In 2007, to facilitate information-security compliance, management formed two dedicated compliance teams, one led by the acting head of TIP and the other led by a high-level IT-security manager within TTS. This compliance structure for information security remained in place through 2013.

Target's primary security-compliance obligations included HIPAA, GLBA, and PCI DSS. The Audit Committee received regular reports on Target's compliance efforts, including PCI DSS compliance, which was the primary compliance obligation for payment card security. As required by the card brands, since 2008 Target has used an independent company as its Qualified Security Assessor to perform the annual PCI DSS security assessment. The annual assessment took more than six months from start to finish. Target was first certified as PCI DSS compliant in 2008 and has received recertification every year since. In 2013, Target received the report from its Qualified Security Assessor that it was PCI DSS compliant on September 20, 2013, approximately two months before the breach began.

3. ***Third-Party Consulting***

In its ongoing efforts to continually assess and improve its security and information protection program, Target sought information from third parties on the state of its cybersecurity program, including its policies, protocols, and systems. To that end, Target engaged Deloitte & Touche LLP to assess Target's maturity in the information security, privacy, and records and information management fields. Deloitte & Touche LLP issued a report to Target in April 2013.

Additionally, Target engaged The Chertoff Group to conduct an evaluation of Target's cybersecurity strategy, governance, network architecture, technology, operations, and the

coordination between security and business units at Target. Chertoff delivered its final report on October 10, 2013. Target management reviewed and considered each of the firms' recommendations contained in their respective reports. The third-party perspectives helped inform Target's planning for existing and planned information protection practices.

G. Data Security Spend and Headcount

Although data-security-specific spend and headcount are not easily quantified, the SLC gained a general understanding of the amount Target spent on data security and the number of security-focused personnel it employed.[40]

Target invested significant capital and resources from 2007 through 2013 in security technology, personnel, and processes. In 2007, Target spent roughly $29 million on data security, including project investments and payroll expenses for security-related personnel. By 2013, Target's annual spending had more than doubled and was upwards of $60 million. Target's investments in security projects over the years included: vulnerability scanning expansion; threat and vulnerability management capabilities; internal and external penetration testing; PCI DSS compliance efforts; enhanced security monitoring; enhanced malware detection software; egress filtering; security tools; data loss prevention; identity and access management; vendor assessments; training; and forensics. The total amount Target invested in security projects from 2007 through 2013 exceeded $200 million. In total, Target spent over $300 million on data security from 2007 through 2013.

From 2010 to 2013, the number of full-time employees dedicated to data security and information protection in TIP and ISI rose from 41 full-time employees to 109 full-time

[40] Target does not report data-security-related expenses on its income statement as a separate line item, nor does it report data security project investments separately on its balance sheet. The numbers discussed here have not been audited, but the SLC has based them on credible evidence gathered during its investigation.

employees. Including TTS and contractors, Target had over 300 people working on security at the time of the breach.

H. Pre-Breach Board Governance

At the time of the data breach, Target's Board of Directors consisted of twelve members elected annually by the shareholders for terms of one year. Eleven of the members were independent, non-management directors. The twelfth was Target's then Chairman, Chief Executive Officer, and President, Gregg Steinhafel. The Board had five committees: Audit, Finance, Compensation, Nominating and Governance, and Corporate Responsibility.

The Audit Committee's responsibility at the time of the breach included assisting the Board of Directors in monitoring the integrity of Target's financial statements, monitoring the independence, qualifications, and performance of Target's independent auditor, monitoring the performance of Target's internal audit function, and monitoring Target's compliance with legal and regulatory requirements. It was also responsible for risk management and risk assessment. Before the breach, the responsibility for data security oversight resided principally with the Audit Committee. At the time of the data breach, the Audit Committee consisted of the following members: Roxanne Austin (Chair), Mary Minnick, Anne Mulcahy, and Derica Rice.[41]

The Finance Committee was responsible for assisting the Board of Directors in examining Target's financial policies and ensuring that Target's finances supported its long-range objectives. The Finance Committee consisted of the following directors at the time of the data breach: Derica Rice (Chair), Roxanne Austin, John Stumpf, and Henrique De Castro.

The Compensation Committee reviewed the compensation of the Board of Directors, the Chief Executive Officer, and other Target executive officers. It gave recommendations to the

[41] A full list of committee assignments at the time of the data breach is attached as Appendix H.

full Board regarding the principal elements of the directors' compensation and made recommendations as to the CEO's performance and the principal elements of the CEO's compensation to the independent directors for approval. The Compensation Committee retained a compensation consultant, Semler Brossy Consulting Group, to assist the Committee in making its recommendations to the full Board. The committee also reviewed and approved the compensation programs for executive officers below the CEO level. At the time of the data breach, the Compensation Committee consisted of the following directors: James Johnson (Chair), Calvin Darden, John Stumpf, and Douglas Baker.

The Nominating and Governance Committee was responsible for ensuring Target had a sufficiently strong Board to assist Target in achieving its short- and long-term goals. It developed the corporate governance principles applicable to Target, monitored the adequacy of their implementation, and oversaw the evaluation of the Board and its committees. The Nominating and Governance Committee consisted of the following directors at the time of the breach: Anne Mulcahy (Chair), Douglas Baker, Calvin Darden, Solomon Trujillo, and Kenneth Salazar.

The Corporate Responsibility Committee reviewed and evaluated Target's public affairs, community relations, corporate social responsibility, and reputation management programs. It was primarily responsible for assessing and overseeing Target's management of reputational risk. The Corporate Responsibility Committee had data security oversight responsibilities as it pertained to the privacy of customers' information and the impact a security breach would have on Target's reputation. At the time of the data breach, the committee's membership consisted of the following directors: Solomon Trujillo (Chair), Calvin Darden, Henrique De Castro, James Johnson, Mary Minnick, and Kenneth Salazar.

X. Target's Post-Breach Modification of its Information Security Program

After the breach, Target made a number of changes to its information security program. High-level summaries of some of the changes are included below. Some of these changes were influenced by the breach, but some were planned before the breach, including projects that had previously had funds allocated for a later time period but were accelerated after the breach. This report does not go into great detail on specific technical changes Target made, not only because the company's controls are continually being changed in the on-going course of business, but also because such specificity would imprudently create risks for the company. *See* SEC Disclosure Guidance: Topic No. 2, (Oct. 13, 2011) ("We are mindful of potential concerns that detailed disclosures could compromise cybersecurity efforts -- for example, by providing a 'roadmap' for those who seek to infiltrate a registrant's network security -- and we emphasize that disclosures of that nature are not required under the federal securities laws.").[42]

A. Post-Breach Technical Enhancements

In the aftermath of the data breach, Target undertook a number of technical projects to strengthen the network and protect customer information. The projects were triaged into short, medium, and long-term priorities. The steps that the company took to strengthen the technical network include the following:

- immediately shutting down the attack path the hacker used;
- forcing resets of a broad number of passwords for employees and vendors;
- expanding the use of password vaults;
- revising remote access procedures;
- further compartmentalizing vendors' access to Target's systems;

[42] *Available at* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

- expanding the use of two-factor authentication;
- reducing or eliminating the access privileges of certain accounts;
- removing certain software from the network;
- enhancing the monitoring and logging of network activity and performing additional network scanning and testing;
- strengthening the segmentation between different portions of the network;
- implementing application whitelisting[43] on point-of-sale systems;
- expanding the use of advanced threat detection tools, creating additional alert rules, and changing the method by which the company responds to alerts; and
- expanding the use of egress filtering.

Target also publicly supported an ongoing industry-wide push for the United States retail and payment card industries to more promptly adopt chip-and-pin or chip-and-sign card technology to replace the United States' historical standard, which was swipe-and-sign.[44] If widely adopted by card issuers and merchants, chip-based cards foster a safer industry-wide payment card system for card-present transactions through the use of the encrypted chip. Target spent roughly $100 million after the breach upgrading its point-of-sale systems to be compatible with chip technology.

B. Post-Breach Administrative and Structural Changes

Target conducted what it referred to as a "Cyber Security Surge" in 2014. Through the Cyber Security Surge, Target reshaped its data security teams and re-prioritized data security projects to focus on those that management deemed tactically critical. Target also created a team

[43] A "whitelist," like a "blacklist," is a general method to manage security. In this context, "application blacklisting" is an approach by which an administrator names which computer processes are not allowed to run on its system. "Application whitelisting" is an alternative approach by which an administrator names specific computer processes that can run on its system and denies access to all others.

[44] Target made an unsuccessful push for chip technology in the early 2000s but abandoned the effort because it was not getting widespread adoption. Chip technology is not practical unless widely adopted by card issuers and merchants.

to address high-priority security and compliance issues. In 2014, Target also restructured the corporate teams responsible for addressing information security concerns. Target did so by gathering employees with security roles from around the enterprise and having them all report to the Chief Information Security Officer (CISO). At the same time, Target made the CISO an officer-level position, where previously the CISO's duties had been managed at the senior director level. The CISO reports to the CIO. Target also reorganized the manager-level employees and contractors reporting through these structures and hired or promoted employees to fill these roles where needed. Target also made an effort to further incorporate information security concerns into the business structure.

In addition to these changes, Target disbanded the SOC and rebuilt it as a new Cyber Fusion Center (CFC) after the breach. The CFC includes a greater array of teams than the SOC housed, including:

- the Cyber Threat Intelligence team, which monitors and assesses potential cyber threats;
- the Cyber Security Incident Response team, which addresses direct threats to the company and analyzes and responds to alerts;
- the Security Testing Services team, which evaluates both new and existing technical programs to incorporate them securely into the Target infrastructure;
- the Red team, Target's group of ethical hackers that simulate real-world cyber-attacks; and
- the Continuous Improvement team, which helps coordinate work between teams within and outside the CFC, helps manage and prioritize work, and records results of that work.

Although elements of these teams were present in Target's information security structure pre-breach, through the creation of the CFC, Target restructured the way it tracks, manages, and responds to security concerns. Target also restructured its incident response plan. The CFC is in regular contact with representatives of external organizations, including government officials. Leaders of the CFC report to the CISO.

C. Post-Breach Personnel Changes

Since the breach, Target has experienced substantial turnover in its information security management personnel. Beth Jacob, Target's CIO, resigned on March 5, 2014. Target then hired Bob DeRodes as interim CIO and Executive Vice President on April 29, 2014. He served in this role until a permanent replacement, Mike McNamara, Tesco PLC's former CIO, was hired on February 3, 2015.[45] DeRodes's role included supervision of the Target Technology Services team, Target's technology operations, and Target's efforts to revamp its data security program. DeRodes also helped the Company shape its long-term information technology roadmap.

During DeRodes's tenure, Target hired Brad Maiorino, the former General Motors CISO and Information Technology Risk Officer. Maiorino became a Target Senior Vice President and its CISO effective June 16, 2014. Maiorino remains in this role as a Senior Vice President as of the date of this Report. The CISO oversees Target's information security teams, develops technology risk strategies, and helps protect Target from external and internal information security threats.

On May 5, 2014, Gregg Steinhafel resigned as CEO, President, and Chairman of the Board of Directors. At the time of Steinhafel's resignation, he and the Board agreed that it would be wise for him to continue to consult with Target in an advisory capacity until August 2014 while John Mulligan adjusted to his additional role as interim President and CEO. Roxanne Austin, then Chair of the Audit Committee, served as the interim Chair of the Board. These interim roles lasted until Brian Cornell joined Target on August 12, 2014 and stepped into the roles of CEO, President, and Chair of the Board. Mulligan remained CFO until September 1,

[45] Tesco PLC is a United Kingdom-based retailer.

2015, when he was promoted to the newly-created position of Chief Operating Officer. Cathy Smith, formerly of Express Scripts, was hired to fill the CFO position.

In the years following the breach, Target also made various personnel changes in the mid- and lower-level management positions responsible for managing and implementing data security. The Company's efforts included hiring new personnel, laying off some personnel, and restructuring and changing existing positions.

D. Post-Breach Reporting and Oversight Changes

During 2014, management began its effort to restructure officer-level management and reporting systems. Jacqueline Rice, formerly the Chief Compliance Officer of General Motors, was hired as a Senior Vice President and Target's Chief Risk and Compliance Officer (CRCO) effective December 1, 2014. The CRCO is responsible for Target's enterprise risk management, compliance, vendor management, and corporate security functions. The CRCO reports to the CEO and the Risk and Compliance Committee of the Board.

Before this position was created, Target's internal audit (then called Assurance) and compliance assessment branches reported to the CFO and the Audit Committee. When the CRCO position was created, Target moved the compliance function, along with Target's enterprise risk management, vendor management, and corporate security functions, under the purview of the CRCO. The internal audit function continues to report to the CFO.

Target also restructured its cyber risk assessment program. Maiorino chairs a committee that focuses on information security risks. That committee, along with others, provides reports to the Enterprise Risk Committee that considers and helps address the company-wide risk profile. Ms. Rice chairs the Enterprise Risk Committee.

E. 2015 Board Governance Restructuring

Target's Board of Directors has also changed since the breach. Two directors, Target's former Lead Independent Director and the former Chair of the Corporate Responsibility Committee, retired from the Board as required by term limits, and four new directors joined Target's Board. Target's Board currently consists of fourteen members who are elected annually by the shareholders for terms of one year. Thirteen of the members are independent, non-management directors, and the fourteenth is Target's Chairman, President, and CEO, Brian Cornell. The Board follows the Corporate Governance Guidelines most recently revised in November 2015. The Board holds five regular meetings each year. Following the data breach—during fiscal year 2014—the Board instead met 11 times. At each regularly scheduled Board meeting, the independent directors meet in executive session without management present. The Board, and each committee, may engage outside counsel, accountants, experts, and other advisors for assistance as necessary.

In early 2015, and again in the fall of 2015, the Board restructured its committees and the allocation of its oversight responsibilities. The most recent changes to the committees are as follows: the Audit Committee and the Finance Committee merged into a single committee; the Compensation Committee added the responsibility for succession planning; the Infrastructure and Investment Committee, a newly-created committee, assumed the responsibility for evaluating Target's investments; and the newly-created Risk and Compliance Committee assumed the responsibility for overseeing Target's risk management and its compliance programs. As a result of the structural changes, the Board now has the following five standing committees: Audit and Finance, Human Resources and Compensation, Nominating and Governance, Risk and Compliance, and Infrastructure and Investment.

The chair of each committee regularly updates the full Board regarding the content of his or her respective committee meetings. The CEO, Target's senior management, or other pertinent Target representatives also report to the Board as appropriate. Target's legal team keeps the Board informed on significant litigation involving Target.

In addition to the duties set forth below, both the Risk and Compliance and the Audit and Finance Committees have roles in data security oversight. The Risk and Compliance Committee oversees the company's risk tolerance determinations, risk governance framework, and risk management policies and procedures. The Audit and Finance Committee retains a role in Target's information security framework by both reviewing the status of the company's internal controls over financial reporting and through the Committee's financial reporting oversight function.

The newly-merged Audit and Finance Committee assists the Board in overseeing Target's financial reporting, the performance of Target's independent auditor, the performance of Target's internal audit function, Target's financial policies and financial risks, and (in coordination with Target's Risk and Compliance Committee) Target's compliance with legal and regulatory requirements. The Audit and Finance Committee oversees Target's financial reporting, internal controls, and financial risks. As mentioned above, it retains a portion of data security oversight responsibility through these functions.

The Risk and Compliance Committee assists the Board in overseeing Target management's identification and evaluation of Target's enterprise risks, including Target's risk management framework and ethics and compliance programs. The Risk and Compliance Committee consists of five committee members, four of whom chair one of the four other standing committees, and the Risk and Compliance Committee Chair, giving this Committee an

enterprise-wide view of risks. The Committee is responsible for providing risk assessment and risk management oversight by engaging management and the full Board with respect to Target's principal operating, business, and compliance risks, including information security risks. The full Board is responsible for overseeing Target's key strategic risks as well as Target's reputation and corporate social responsibility efforts.

The Human Resources and Compensation Committee assists the Board with employee compensation and has the authority to retain a compensation consultant. The Committee, with the assistance of the retained consultant, annually reviews the CEO's performance and recommends how the full Board should determine the principal elements of the CEO's compensation. The Committee also reviews and approves the compensation programs for other executive officers. The Committee maintains oversight responsibility for Target's risks related to compensation, organizational talent, Target culture, and risks related to management succession. The Committee also determines director compensation.

The Infrastructure and Investment Committee oversees Target's investment activity and evaluates Target's strategic investment decisions. It is responsible for overseeing investment risks, including those related to Target's capital expenditures, major expense commitments, and infrastructure needs.

The Nominating and Governance Committee oversees the evaluation of the Board and its committees, identifies individuals qualified for election as directors, develops corporate governance guidelines, and provides oversight over Target's policies and practices regarding public policy advocacy and political activities. It is also responsible for overseeing governance structuring and Board succession.

XI. Core Legal Principles

In evaluating the merits of the claims asserted against the directors and officers, the SLC considered the law governing those claims, potential defenses, and the effect of indemnification and exculpation. The following is a summary of certain core legal principles governing the claims asserted in the Demand and derivative actions. The summary should not be considered all-inclusive or determinative; rather, it sets a framework for the SLC's consideration of the relevant issues.

A. Law Governing Proceedings of an SLC

The law of the state of incorporation determines the authority a special litigation committee has to address a derivative action. *See Burks v. Lasker*, 441 U.S. 471, 486 (1979) ("federal courts should apply state law governing the authority of independent directors to discontinue derivative suits."). In Minnesota, a board of directors may create a special litigation committee "consisting of one or more independent directors or other independent persons to consider legal rights or remedies of the corporation and whether those rights and remedies should be pursued." Minn. Stat. § 302A.241, Subd. 1; *In re UnitedHealth Group Inc. S'holder Derivative Litig.*, 754 N.W.2d 544, 550 (Minn. 2008). Members of a special litigation committee do not need to be directors. Minn. Stat. § 302A.241, Subd. 2. "Committees other than special litigation committees . . . are subject at all times to the direction and control of the board." Minn. Stat. § 302A.241, Subd. 1. Thus, by statute, an SLC is not subject to a board's direction and control. *See id.*; *In re UnitedHealth Group Inc. S'holder Derivative Litig.*, 754 N.W.2d 544, 550 (Minn. 2008)

In the seminal Minnesota Supreme Court case governing SLCs, *Janssen v. Best & Flanagan*, 662 N.W.2d 876, 889 (Minn. 2003), the Court stated that a special litigation

committee is expected to undertake a "comprehensive weighing and balancing of factors" that takes into account the legal, ethical, commercial, promotional, professional, public relations, fiscal, and other factors "common to reasoned business decisions," thus establishing that an SLC must make a business judgment about whether to pursue certain claims, not just a legal one. Five years later, in a question certified to it by the United States District Court for the District of Minnesota, the Minnesota Supreme Court, in *In re UnitedHealth Group Inc. Shareholder Derivative Litigation*, determined the degree of deference a court should give to a special litigation committee's decision. The Court held that under the Minnesota business judgment rule, a court must defer to a special litigation committee's decision with respect to a shareholder derivative action if the proponent of that decision demonstrates that (1) the members of the SLC possessed a disinterested independence and (2) the SLC's investigative procedures and methodologies were adequate, appropriate, and pursued in good faith. 754 N.W.2d at 561.

B. Legal Principles Applicable to the Demand and Derivative Complaints

1. Standard of Conduct, Exculpation, and Indemnification

a. Fiduciary Duties of Directors

Directors have two primary fiduciary responsibilities: the duty of loyalty and the duty of care. The Minnesota Business Corporation Act (MBCA), codified in chapter 302A of the Minnesota Statutes, requires directors to "discharge the duties of the position of director in good faith, in a manner the director reasonably believes to be in the best interests of the corporation, and with the care an ordinarily prudent person in a like position would exercise under similar circumstances…." Minn. Stat. § 302A.251, Subd. 1. "Good faith" is defined as "honesty in fact in the conduct of the act or transaction concerned." Minn. Stat. § 302A.011, Subd. 13. "A

person who so performs those duties is not liable by reason of being or having been a director of the corporation." *Id.*

When directors in good faith comply with the duties of loyalty and care, their decisions are protected by the business judgment rule. "The business judgment rule is a presumption developed by state and federal courts to protect boards of directors against shareholder claims that the board made unprofitable business decisions." *In re UnitedHealth Group Inc. S'holder Derivative Litig.*, 754 N.W.2d at 551 (internal quotation marks omitted). Under the business judgment rule, as long as a disinterested director makes "an informed business decision, in good faith, without an abuse of discretion, he or she will not be liable for corporate losses resulting from his or her decision." *Id.*; *see also* Minn. Stat. § 302A.251, Subd. 1; *Janssen*, 662 N.W.2d at 882 (recognizing application of business judgment rule where disinterested directors make an informed business decision in good faith and without an abuse of discretion, in part on the grounds that "courts are ill-equipped to judge the wisdom of business ventures and have been reticent to replace a well-meaning decision by a corporate board with their own") (citation omitted). When directors fail to comply with either of these duties, they are not entitled to the protection of the business judgment rule and may be held liable for damages. *Foy v. Klapmeier*, 992 F.2d 774, 780 (8th Cir. 1993) ("Under Minnesota law an officer or director is personally liable for all damages caused by self-dealing in breach of his or her fiduciary obligations.").[46]

The MBCA further provides that directors, in discharging their duties, can rely on information provided by others. Specifically:

[46] Under Minnesota law, however, a resolution fixing directors compensation is not self-dealing. Minn. Stat. § 302A.255, Subd. 2(a). Such a resolution is not void or voidable and does not give rise to a conflict of interest because it is excluded under Minn. Stat. § 302A.255. *See also* Minn. Stat. 302A.211 ("Subject to any limitations in the articles or bylaws, the board may fix the compensation of directors.").

> A director is entitled to rely on information, opinions, reports, or statements, including financial statements and other financial data, in each case prepared or presented by:
>
> (1) one or more officers or employees of the corporation whom the director reasonably believes to be reliable and competent in the matters presented;
>
> (2) counsel, public accountants, or other persons as to matters that the director reasonably believes are within the person's professional or expert competence; or
>
> (3) a committee of the board upon which the director does not serve … as to matters within its designated authority, if the director reasonably believes the committee to merit confidence.

Minn. Stat. § 302A.251, Subd. 2(a). Each of the above-described scenarios have a reasonableness component attached to the director's reliance. *See id.* A director is not entitled to rely on others, however, if the director "has knowledge concerning the matter in question that makes the reliance otherwise permitted by [subdivision 2(a)] unwarranted." Minn. Stat. § 302A.251, Subd. 2(b).

Under Minnesota law, directors have two layers of protection against breaches of the duty of due care. Minnesota law allows a Minnesota corporation to provide for exculpation, and in the absence of explicit language in the articles or bylaws, mandates indemnification of a director for breach of the duty of due care, though not the duty of loyalty.

As to exculpation, the MBCA provides that "[a] director's personal liability to the corporation or its shareholders for monetary damages for breach of fiduciary duty as a director may be eliminated or limited in the articles." Minn. Stat. § 302A.251, Subd. 4. This section also establishes, however, that the articles "shall not eliminate or limit the liability of a director" in the following circumstances:

> (a) for any breach of the director's duty of loyalty to the corporation or its shareholders;
>
> (b) for acts or omissions not in good faith or that involve intentional misconduct or a knowing violation of law;

> (c) under section 302A.559 [liability of directors for illegal distributions] or 80A.76 [civil liability for breach of the anti-fraud provisions of the Minnesota securities regulation statute];
> (d) for any transaction from which the director derived an improper personal benefit; or
> (e) for any act or omission occurring prior to the date when the provision in the articles eliminating or limiting liability becomes effective.

Id.

Target's articles of incorporation explicitly provide for exculpation of directors. Therefore, if the statutory conditions are met, Target directors cannot be held personally liable for monetary damages for breach of fiduciary duty to Target or its shareholders.

As noted, Minnesota law also mandates indemnification of present and former directors acting in their official capacity, provided the corporation's articles or bylaws do not provide otherwise and the activities meet the standard of conduct established by Minn. Stat. § 302A.521. In a civil case, unless the articles of incorporation or bylaws prohibit indemnification, the statutory standard of conduct requires indemnity where the individual:

(1) has not been indemnified by another entity for the same judgment and with respect to the same acts or omissions;

(2) acted in good faith;

(3) received no improper personal benefit; and

(4) reasonably believed the conduct was in the best interests of the corporation.

Minn. Stat. § 302A.521, Subd. 2.

Target's bylaws and articles of incorporation do not limit the statutory rights of indemnification or advances. In fact, the bylaws, in referring to Minn. Stat. § 302A.521, explicitly allow for indemnification to the fullest extent. Thus, by meeting this statutory standard, a director, officer, or employee is entitled to indemnification from Target for fees,

costs, and judgment in an action initiated by the corporation or a shareholder's derivative action. *See* Minn. Stat. § 302A.521, Subd. 1(d) (including "a proceeding by or in the right of the corporation" as a proceeding indemnifiable by statute).[47]

b. Fiduciary Duties of Officers

Officers are subject to much the same standard of conduct as directors, with a few differences. Reporter's Notes, Minn. Stat. Ann. § 302A.361 (West). The statutory language describing the standard of conduct for officers states: "An officer shall discharge the duties of an office in good faith, in a manner the officer reasonably believes to be in the best interests of the corporation, and with the care an ordinarily prudent person in a like position would exercise under similar circumstances." *Id.*; *compare* Minn. Stat. § 302A.361 *with* Minn. Stat. § 302A.251, Subd. 1. Among the statutory differences between directors and officers is that the officers' right of reliance upon others is more circumscribed than the directors' right of reliance upon others. Reporter's Notes, Minn. Stat. Ann. § 302A.361. An officer "has no right simply to rely on information provided by another person if the matter relied on is within that officer's own area of direct responsibility. … [T]hat officer may have a right to rely on others if the matter is outside the scope of the relying officer's responsibility." *Id.* If an ordinarily prudent person in the officer's position would have relied on an expert's opinion or on a subordinate as to a matter that is not, and should not be, the officer's primary responsibility, reasonable reliance should be permitted under the general statutory standard set forth in section 302A.361. *Id.*

[47] Section 302A.521, Subd. 3 also provides that a director or a party to a derivative proceeding is entitled to advances for fees and costs incurred in such proceeding. To be entitled to advances, a director must provide an undertaking to repay the company all amounts if it is later determined the criteria for indemnification has not been satisfied and a determination that the facts then known to those making the determination would not preclude indemnification. Minn. Stat. § 302A.521, Subd. 3.

Unless prohibited by a company's articles of incorporation or bylaws, officers are permitted, under section 302A.351, to delegate some or all of the duties of an office to other persons without board approval. An officer delegating the duties or powers of an office retains the duty to supervise the subordinate. The delegating officer is subject to the standard of conduct for an officer stated in section 302A.361, discussed above, with respect to (1) the act of delegation and (2) the supervision of persons to whom those duties and powers are so delegated. Minn. Stat. § 302A.351. That is to say, both the act of delegation and the supervision of the subordinate must be done in good faith and in a manner the officer reasonably believes to be in the best interests of the corporation and with the care an ordinarily prudent person in a like position would exercise. Neither Target's articles of incorporation nor the bylaws prohibit the statutory rights of delegation.

Target's officers and employees, like its directors, are protected by mandatory statutory indemnification under Minn. Stat. § 302A.521 (*see* discussion, *supra* at Part XI.B.1.a).

2. Oversight Responsibility Generally

No reported case involving the oversight responsibilities of directors of a Minnesota corporation has been decided to date. In the past, Minnesota courts have often looked to the decisions of Delaware courts for guidance in the area of corporate and business law. *See In re Xcel Energy, Inc.*, 222 F.R.D. 603, 606 (D. Minn. 2004); *Markewich ex rel. Medtronic, Inc. v. Collins*, 622 F. Supp. 2d 802, 808 (D. Minn. 2009); *Haberle ex rel. Gander Mountain Co. v. Baker*, 2005 WL 2105543, at *3 (D. Minn. Aug. 30, 2005). However, Minnesota courts have specifically refused to "adopt blindly" the Delaware approach as doing so in certain situations would be "at odds with general principles of Minnesota law." *Haberle* at *3.

Under the applicable Minnesota statute, "[t]he business and affairs of a corporation [are to] be managed by or under the direction of a board." Minn. Stat. § 302A.201. By Minnesota statute and with Delaware courts as a guide, the board of a Minnesota corporation likely would be required under Minnesota law to have a significant oversight role. In *In re Caremark International Inc. Derivative Litigation*, the leading Delaware case on director oversight liability, the Delaware Court of Chancery explained that a board's oversight role includes a duty to attempt in good faith to assure that an adequate corporate information and reporting system exists and that it is "reasonably designed to provide to senior management and to the board itself timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning both the corporation's compliance with law and its business performance." 698 A.2d 959, 970 (Del. Ch. 1996); *see also In re Johnson & Johnson Derivative Litig.*, 865 F. Supp. 2d 545 (D.N.J. 2011) (adopting the *Caremark* standard in New Jersey); *In re Abbott Labs. Derivative S'holders Litig.*, 325 F.3d 795 (7th Cir. 2003) (scrutinizing Illinois corporation directors under the *Caremark* standard). In *Caremark*, the plaintiffs claimed that the defendant directors breached their fiduciary duty for having "allowed a situation to develop and continue which exposed the corporation to enormous legal liability and that in so doing they violated a duty to be active monitors of corporate performance." *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d at 967. The court noted that holding directors liable for an alleged breach of care in this oversight capacity "is possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment." *Id.*

In *Stone ex rel. AmSouth Bancorporation v. Ritter*, 911 A.2d 362, 365 (Del. 2006), the Delaware Supreme Court approved the *Caremark* standard, holding that it articulates the necessary conditions for director oversight liability. The standard then, as articulated in *Stone*,

for director oversight liability requires a showing that "(a) the directors utterly failed to implement any reporting or information system or controls; *or* (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention." *Id.* at 370 (emphasis in original). In both cases, imposition of liability requires a showing that the directors knew that they were not discharging their fiduciary obligations. *Id.*

3. Gross Mismanagement, Abuse of Control, and Duty of Candor

The Eighth Circuit has alluded to a claim of gross mismanagement under Minnesota law but analyzed the mismanagement claim under traditional breach of fiduciary duty standards. *See, e.g.*, *Earle R. Hanson & Assocs. v. Farmers Coop. Creamery Co. of Clear Lake, Wis.*, 403 F.2d 65, 69-70 (8th Cir. 1968) (applying Minnesota law). Further, at least three courts from other jurisdictions, in the context of shareholder derivative suits, have held that claims of abuse of control and gross mismanagement, among others, were not separate claims but rather premised on the breach of fiduciary duty claim. *See Clark v. Lacy*, 376 F.3d 682, 686–87 (7th Cir. 2004) (referring to plaintiff's abuse of control, gross mismanagement, and waste of corporate assets claims as "repackaging the same issue under different causes of action"); *In re Zoran Corp. Derivative Litig.*, 511 F. Supp. 2d 986, 1019 (N.D. Cal. 2007) (although the court allowed fiduciary duty claim to proceed, summary judgment for defendants on claims of abuse of control, gross mismanagement, constructive fraud, and rescission was granted because such claims were considered "a repackaging of claims for breach of fiduciary duties instead of being a separate tort"); *In re Citigroup Inc. S'holder Derivative Litig.*, 964 A.2d 106, 115 n. 6 (Del. Ch. 2009) ("Delaware law does not recognize an independent cause of action against corporate directors and officers for reckless and gross mismanagement; such claims are treated as claims

for breach of fiduciary duty."). In the context of the Demand and complaints here, the language of gross mismanagement and abuse of control fall under the breach of fiduciary duty category of claims.

Collier further alleges a breach of the "duty of candor." Courts analyzing Minnesota law have not explicitly defined this duty but instead analyze it as existing, if at all, as a part of another fiduciary duty. *See, e.g.*, *Gunderson v. Alliance of Computer Prof'ls, Inc.*, 628 N.W.2d 173, 186 (Minn. Ct. App. 2001) (stating, in the context of a closely held corporation, the duty of loyalty encompasses the duty of candor), *review granted* (Minn. July 24, 2001), *appeal dismissed* (Minn. Aug. 17, 2001).

Under Delaware law, the duty of candor only exists separately from the duties of care and good faith to the extent it "entails the obligation to disclose all material information to shareholders when seeking shareholder approval." *Potter v. Pohlad*, 560 N.W.2d 389, 395 (Minn. Ct. App. 1997) (applying Delaware law). The Delaware Supreme Court commented that the duty of candor "represents nothing more than the well-recognized proposition that directors of Delaware corporations are under a fiduciary duty to disclose fully and fairly all material information within the board's control when it seeks shareholder action." *Stroud v. Grace*, 606 A.2d 75, 84 (Del. 1992) (further referring to the use of the term duty of candor as "confusing and imprecise given the well-established principles and duties of disclosure that otherwise exist.").

4. ***Corporate Waste***

Under Minnesota law, a court is authorized to "grant any equitable relief it deems just and reasonable in the circumstances" or "dissolve a corporation and liquidate its assets and business [if] the corporate assets are being misapplied or wasted." Minn. Stat. § 302A.751, Subd. 1(b)(5). "The essence of a claim of waste of corporate assets is the diversion of corporate

assets for improper or unnecessary purposes." *Michelson v. Duncan*, 407 A.2d 211, 217 (Del. 1979). To establish a corporate waste claim, facts must be shown that "no person of ordinary sound business judgment could view the benefits received in the transaction as a fair exchange for the consideration paid by the corporation." *Harbor Fin. Partners v. Huizenga*, 751 A.2d 879, 892 (Del. Ch. 1999) (citation omitted); *see also Glazer v. Zapata Corp.*, 658 A.2d 176, 183 (Del. Ch. 1993) (referring to exchange that is "so one sided that no business person of ordinary, sound judgment could conclude that the corporation has received adequate consideration."). Waste is "an extremely difficult claim to prove." *Telxon Corp. v. Bogomolny*, 792 A.2d 964, 975 (Del. Ch. 2001); *see also Postorivo v. AG Paintball Holdings, Inc.*, 2008 WL 553205, *9 n. 42 (Del. Ch. Feb. 29, 2008) (noting that although the standard for demonstrating waste is not an "impossible" one to meet, "merely poor, misguided, or loss-making transactions are insufficient for a finding of waste") (citation omitted).

5. Restitution

Restitution is the remedy for unjust enrichment of the defendant at the plaintiff's expense. *United Prairie Bank-Mountain Lake v. Haugen Nutrition & Equip., LLC*, 813 N.W.2d 49, 58 (Minn. 2012) (citing 1 Dan B. Dobbs, *Law of Remedies* § 4.1(1) at 551–52 (2d ed. 1993) ("[R]estitution claims are bound by a major unifying thread. Their purpose is to prevent the defendant's unjust enrichment by recapturing the gains the defendant secured in a transaction.")); *Randall v. Constans*, 23 N.W. 530, 533 (Minn. 1885) (holding that a plaintiff may seek restitution against a defendant who was unjustly enriched). In general, therefore, restitution is based on a benefit that has been conferred on the defendant, rather than a loss incurred by the plaintiff. *United Prairie Bank-Mountain Lake*, 813 N.W.2d at 58 (citing Dobbs, *supra*, § 4.1(1), at 555 ("Restitution measures the remedy by the defendant's gain and seeks to force

disgorgement of that gain. It differs in its goal or principle from damages, which measures the remedy by the plaintiff's loss and seeks to provide compensation for that loss.")).

6. Securities Misrepresentation

Parties who are neither buyers nor sellers of securities but who claim securities law violations must bring their claims derivatively. *City Nat'l Bank of Fort Smith, Ark. v. Vanderboom*, 422 F.2d 221, 228 (8th Cir. 1970). To establish a breach of fiduciary duty in connection with alleged misrepresentations under securities laws, a corporation suing its directors must first prove a primary violation. Under the governing case law, to prove a federal fraud claim under Rule 10b-5, the plaintiff must prove the following: (1) a material misrepresentation or omission; (2) scienter; (3) a connection between the misrepresentation or omission and the purchase or sale of a security; (4) reliance upon the misrepresentation or omission; (5) economic loss; and (6) loss causation. *Amgen Inc. v. Conn. Ret. Plans & Trust Funds*, 133 S. Ct. 1184, 1191–92 (2013). To be actionable, a statement must be materially misleading. *Basic Inc. v. Levinson*, 485 U.S. 224, 239 n.17 (1988). Silence, absent a duty to disclose, is not misleading. *Id.*

XII. Factors Taken into Consideration by the SLC

The SLC investigated and took into consideration all the allegations in the Demand and derivative complaints. The SLC also sought to determine whether there were other rights Target could properly assert and whether pursuing any claims arising from the data breach would be in Target's best interests. In reaching its conclusions, the SLC considered the legal and factual

strengths and weaknesses of all of the claims. It also undertook a comprehensive weighing and balancing of numerous factors, including the following:[48]

- the financial expenditures required to litigate the claims, including Target's obligations to indemnify and advance defense costs;
- the existence of the exculpation clause in Target's Articles of Incorporation and the statutory rights of indemnification;
- contractual and legal issues relating to Target's Directors and Officers Liability insurance coverage for claims of breach of fiduciary duty arising out of the data breach;
- the existence of network-security insurance coverage that mitigated Target's exposure to data-breach-related losses;
- the applicability of the business judgment rule protecting reasonably prudent, good faith business decisions;
- the pre-breach and current economic health of Target, including the trajectory of the stock price, dividends paid to shareholders, and same-store sales figures;
- the effect the breach had on Target's revenues, profits, customer traffic, and stock price and their subsequent recovery;
- the overall cost of the breach, including direct and indirect expenses associated with the breach;
- the pre-breach existence and content of Target's policies and procedures designed to establish a reasonable information security program that incorporated technical, administrative, and physical controls for data security;
- the pre-breach existence and content of Target's compliance policies and procedures and audit procedures designed to test and to assure adherence to those policies and procedures;
- management's reports to the Board's Audit and Corporate Responsibility Committees covering Target's data security program, including compliance efforts and assessments of Target's data security and privacy programs;
- the level of expenditures on data security between 2007 and 2013;
- the level of Target's employees' knowledge of the vulnerabilities exploited during the breach and the efforts and decisions made to address those vulnerabilities;

[48] The factors in this list are not exclusive and are not listed in any particular order. No inferences should be drawn about the weight the SLC applied to any factor based on where it appears in this list.

- the competence and engagement of Target data security management and employees pre- and post-breach;
- Target's pre-breach plans for continuous improvement of its data security systems and controls;
- Target's utilization of third-party experts and consultants to help it evaluate its data security program;
- the role and limitations of PCI DSS compliance in assessing the security of Target's cardholder data environment;
- Target's use of a professional Qualified Security Assessor to assess and render an annual opinion on its compliance with PCI DSS requirements;
- the Qualified Security Assessor's report on Target's compliance with the PCI DSS issued September 20, 2013;
- the efforts of TIP and TTS to attempt to ensure compliance with obligations imposed by government and industry data security standards;
- the history of reports that demonstrate that Target had been assessed as PCI DSS compliant each year since 2008;
- the reports that were made to Target's officers and directors that it had been assessed as PCI DSS compliant, including to the Audit Committee of the Board;
- Target's internal reports of deficiencies in the data security program as revealed in internal memoranda;
- the lack of pre-breach adverse governmental regulatory action by regulators concerning Target's data security program;
- the reports of the independent auditors from Ernst & Young to the Audit Committee and Target management that prior to the breach there were no significant deficiencies or material weaknesses in the information technology general controls, which included security-related information technology general controls;
- Target's post-breach efforts to mitigate the cost and inconvenience of the breach to its customers;
- Target's post-breach remediation of data security vulnerabilities exposed by the breach;
- the resignations of the CEO and CIO in the months following the breach and other personnel changes;
- Target's post-breach corporate governance changes related to risk in general and data security risk in particular, including making the CISO a Senior Vice President position and hiring and installing a Corporate Risk and Compliance Officer who reports to the CEO and to the Board's Risk and Compliance Committee;

- the re-election of the Board of Directors in the period following the breach;
- the rights of officers and directors to reasonably rely on the information and opinions of others, including other officers and directors, committees of the Board, employees, and advisors;
- the requirements necessary to support a finding of liability against the officers and directors, especially in the context of governing statutory and case law;
- Target's efforts from 2007 to the present to strengthen its information security program;
- the recognition by the FTC that the mere fact that a breach occurred does not mean that a company has violated the law;
- the disruption and distraction to Target's ongoing business and the effect on its reputation that could be caused by suing or taking other legal action against past or present officers or directors;
- the effect on employee morale if Target pursued such claims;
- the reasonableness of judgments that Target officers, directors, and employees made concerning whether and when to address capital and employment needs related to data security risks;
- the size, scope, and complexity of Target's technology footprint in addressing data security strategy and needs; and
- Target's corporate culture at the employee, officer, and director levels.

XIII. The SLC's Conclusion

Having concluded its investigation, the SLC has considered these and other factors, has performed a careful weighing and balancing of these factors, and has determined that it is not in Target's best interests to pursue claims against the officers or directors identified in the Demand and derivative complaints. The SLC, through its counsel, will communicate this determination to the Demand and derivative shareholders and will seek dismissal of the derivative complaints.

Dated: March 30, 2016

Respectfully,

The Special Litigation Committee of the
Board of Directors of Target Corporation

John Matheson

Hon. Kathleen Blatz