UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MINNESOTA

MAUREEN COLLIER, Derivatively on Behalf of TARGET CORPORATION, Plaintiff, v. GREGG W. STEINHAFEL, JOHN J. MULLIGAN, BETH M. JACOB, 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, Defendants, -and- TARGET CORPORATION, Nominal Defendant.	Case No. **VERIFIED SHAREHOLDER DERIVATIVE COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Maureen Collier ("Plaintiff"), by and through her attorneys, derivatively on behalf of nominal defendant Target Corporation ("Target" or the "Company"), submits this Verified Shareholder Derivative Complaint against the directors and officers named herein (collectively, the "Individual Defendants"). Plaintiff's allegations are based upon personal knowledge as to herself and her own acts, and upon information and belief developed from the investigation and analysis of her counsel, which includes, among other things, the review of public filings by Target with the U.S. Securities and Exchange Commission ("SEC"), as well as,

press releases, news reports, analyst reports, complaints pending against the Company, and other information available in the public domain.

SUMMARY OF THE ACTION

1. This is a verified shareholder derivative action by Plaintiff on behalf of Target against certain of its officers and members of its Board of Directors (the "Board"), who are disabled from responding to a litigation demand by any Target shareholder because of their insider connections, tenure on the board, and involvement in the alleged wrongdoing for which they face a substantial likelihood of liability.

2. The Individual Defendants' (as defined below) wrongful conduct extends at least from January 1, 2013 to the present (the "Relevant Period"). On behalf of Target, Plaintiff seeks monetary damages and injunctive relief by way of significant corporate and managerial reforms to prevent future harm to the Company by disloyal directors and officers.

3. Target trails Walmart as the second largest general merchandise retailer in the United States. Target allows customers to pay for goods using a variety of methods. A key method of payment in the digital age is via credit or debit card. Credit and debit card purchases are common in Target stores and are the primary method of payment on Target's website for online purchases. Additionally, Target derives a substantial portion of its business through its own proprietary Target credit cards. To complete these transactions, Target routinely collects its customers' personal and financial information. In addition to the information needed to complete a financial transaction, Target also collects vast amounts of other personal information about its customers, even tracking their purchase history to preemptively market potential future purchases. Customers are generally unaware that most of this information is collected and

retained. For the information that customers do willingly submit to complete a purchase, Target assures its customers that it will protect its sensitive and private nature.

4. This action arises out of the Individual Defendants' responsibility for, release of false and misleading statements concerning, and the bungling of the aftermath of the ***worst data breach in retail history***.[1] The Individual Defendants caused Target to violate its express and implied promises to customers by failing to take reasonable steps to maintain its customers' personal and financial information in a secure manner.

5. When the Individual Defendants first revealed the breach, they significantly downplayed its true significance. The initial response from Target was that the breach only concerned data taken from the forty million customers who made credit and debit card purchases in physical Target stores nationwide between November 27 and December 15, 2013. The Individual Defendants also withheld from the public the news of the breach until after the 2013 Holiday Shopping Season in order to preserve sales figures during the most popular shopping period of the fiscal year. The fact that the Individual Defendants withheld the truth about the breach, put millions more customers at risk and had the effect of significantly increasing the damage to Target's goodwill and brand trust.

6. Almost a month after the breach, Target revealed the whole story. Namely, as a result of the Individual Defendants' failure to enact appropriate security measures, identity thieves were able to steal sensitive personal and financial data from as many as one hundred ten million customers who had shopped at Target over the last decade. The Individual Defendants' lack of controls effectively turned the vast majority of Target customers into victims of identity theft.

[1] 'Worst breach in history' puts data-security pressure on retail industry, CNBC, http://www.cnbc.com/id/101328596

7. Identity theft occurs when a thief wrongfully obtains a victim's personal information, without the victim's knowledge, to commit theft or fraud. For many of these victims, identity thieves have already used this personal information to commit fraud and other crimes. The remaining victims are forced to constantly wait and monitor financial and personal records to protect themselves from the threat of identity theft and fraudulent charges being made to their credit and debit card accounts that Target failed to keep safe.

8. In addition to being the ***worst breach in history***, the Individual Defendants aggravated the damage to customers by failing to provide prompt and adequate notice to customers and by releasing numerous statements aimed to create a false sense of security to affected customers. Initially, the Individual Defendants allowed Target to delay admitting the breach to the public until December 19, 2013, several weeks after the breach began and four whole days after it had been contained. Worse, Target disclosed the data breach only after its hand was forced by third-party reports breaking the news. Still, after these mistakes, Target concealed the full breadth and depth of the data breach. In particular, Target initially reported on December 19, 2013 that the data breach affected forty million people and assured those affected by the data breach that "the issue has been identified and resolved," and that there was "no indication that there has been any impact to PIN numbers." Target further reassured worried customers that "someone cannot visit an ATM with a fraudulent debit card and withdraw cash." In fact, Target tried to preserve holiday sales figures and store traffic despite the negative news by offering all customers a 10% discount during the weekend of December 21 and 22, 2013, immediately following the initial disclosure of the breach.

9. Despite these statements to the contrary, just days after Target's initial disclosure of the data breach, news outlets began reporting that encrypted PIN (or personal identification

number) data had been stolen during the breach and that those codes could be used by identity thieves to make fraudulent withdrawals from bank accounts. In response to these allegations, Target continued for several days to deny that any of its customers' PIN data had been compromised.

10. On December 27, 2013, Target finally admitted that customers' PIN data had been compromised in the breach. Following the pattern of initially withholding the full truth until forced to tell all by independent news sources, on January 10, 2014, Target released a statement indicating that the breach had actually affected seventy million additional customers who had shopped at Target over the past ten years, not just the short period during the 2013 holiday shopping season.

11. Even after Target came clean about the true nature and scope of the breach, its customers have not been able to rest easy. To qualm customer fears about identity theft, Target began offering free credit monitoring services to affected customers in the aftermath of the breach. Because Target thought this capitulation would be a good press public relations opportunity, they widely disclosed the credit services. Shortly thereafter, another round of identity thieves capitalized on this new opportunity to exploit Target's customers. In addition to the official emails sent to Target customers, including the proper links to sign up for free credit monitoring, a wider swath of sham emails sent by credit predators was sent out to Target customers and many people who had never even shopped at Target. These emails bore uncanny resemblances to the official emails but had the inverse purpose. The sham emails instructed the recipients to pass along their credit information so that it could be "monitored," when it fact it was just being directly stolen. This secondary breach has further eroded Target's goodwill and customer confidence.

12. The Individual Defendants' failures to implement any internal controls at Target designed to detect and prevent such a data breach, and then to timely report it, have severely damaged the Company. The Company's data breach is currently under investigation by the United States Secret Service ("Secret Service") and the Department of Justice ("DOJ"). The breach is also the subject of hearings in the United States Senate. Defendant John J. Mulligan ("Mulligan"), the Company's Executive Vice President and Chief Financial Officer ("CFO") is scheduled to appear before the Senate Judiciary Committee on February 4, 2014 to answer questions about the worst data breach in history. Finally, there are currently at least nineteen class action lawsuits filed against Target on behalf of affected customers. These class action lawsuits pose the risk of hundreds of millions of dollars in damages to the Company. Plaintiff therefore seeks damages and other relief on behalf of the Company.

JURISDICTION AND VENUE

13. This Court has diversity jurisdiction over this action pursuant to 28 U.S.C. §1332. All defendants are completely diverse from the Plaintiff and the amount in controversy exceeds $75,000.00.

14. This Court has personal jurisdiction over each of the defendants because each defendant is either a corporation conducting business and maintaining operations in this District, or is an individual who is either present in this District for jurisdictional purposes or has sufficient minimum contacts with this District so as to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

15. Venue is proper in this District pursuant to 28 U.S.C. §1391 because (i) one or more of the defendants either resides or maintains executives offices in the District; (ii) a substantial portion of the transactions and wrongs complained of herein occurred in the District;

and (iii) defendants have received substantial compensation and other transfers of money in the District by doing business and engaging in activities having an effect in the District.

PARTIES

Plaintiff

16. Plaintiff is presently a shareholder of Target. Plaintiff has been a shareholder continuously at all times relevant to the claims asserted herein and will remain a shareholder through the conclusion of this litigation. Plaintiff is a citizen of Florida.

Nominal Defendant

17. Nominal Defendant Target is a Minnesota corporation with principal executive offices located at 1000 Nicollet Mall, Minneapolis, Minnesota 55440. Target is publicly traded on the New York Store Exchange under the ticker symbol TGT.

Individual Defendants

18. Defendant Gregg W. Steinhafel ("Steinhafel") has served as Target's Chief Executive Officer ("CEO") since May 2008; President since August 1999; Chairman of the Board since February 2009; and director since 2007. Defendant Steinhafel has been employed by Target since 1979. Defendant Steinhafel is a citizen of Minnesota.

19. Defendant Mulligan has served as Target's Executive Vice President and CFO since April 1, 2012. Defendant Mulligan has served Target in key leadership positions in finance and human resources for over sixteen years. Defendant Mulligan is a citizen of Minnesota.

20. Defendant Beth M. Jacob ("Jacob") has served as Target's Chief Information Officer since July 2008 and Executive Vice President - Target Technology Services since January 2010. Defendant Jacob also served as Senior Vice President - Target Technology Services from July 2008 to January 2010 and Vice President - Guest Operations, Target Financial Services from August 2006 to July 2008. Defendant Jacob is a citizen of Minnesota.

21. Defendant James A. Johnson ("Johnson") has served as Target's Lead Independent Director since April 2012 and as director since 1996. Defendant Johnson has also served as a member of Target's Corporate Responsibility Committee since April 2012. Defendant Johnson is a citizen of Washington, D.C.

22. Defendant Solomon D. Trujillo ("Trujillo") has served as a Target director since 1994. Defendant Trujillo has also served as Chairman of Target's Corporate Responsibility Committee since April 2012. Defendant Trujillo is a citizen of California.

23. Defendant Anne M. Mulcahy ("Mulcahy") has served as a Target director since 1997. Defendant Mulcahy has also served as a member of Target's Audit Committee since at least January 2014. Defendant Mulcahy is a citizen of Connecticut.

24. Defendant Roxanne S. Austin ("Austin") has served as a Target director since 2002. Defendant Austin has also served as Chairman of Target's Audit Committee since April 2012. Defendant Austin is a citizen of California.

25. Defendant Calvin Darden ("Darden") has served as a Target director since 2003. Defendant Darden has also served as a member of Target's Corporate Responsibility Committee since at least January 2014. Defendant Darden is a citizen of Georgia.

26. Defendant Mary E. Minnick ("Minnick") has served as a Target director since 2005. Defendant Minnick has also served as a member of Target's Audit and Corporate Responsibility Committees since April 2012. Defendant Minnick is a citizen of the United Kingdom.

27. Defendant Derica W. Rice ("Rice") has served as a Target director since 2007. Defendant Rice has also served as a member of Target's Audit Committee since April 2012. Defendant Rice is a citizen of Indiana.

28. Defendant John G. Stumpf ("Stumpf") has served as a Target director since 2010. Defendant Stumpf also served as a member of Target's Audit Committee from at least April 2012 until March 2013. Defendant Stumpf is a citizen of California.

29. Defendant Douglas M. Baker, Jr. ("Baker") has served as a Target director since March 2013. Defendant Baker also served as a member of Target's Audit Committee from March 2013 to April 2013. Defendant Baker is a citizen of Minnesota.

30. Defendant Henrique De Castro ("De Castro") has served as a Target director since March 2013. Defendant De Castro has also served as a member of Target's Corporate Responsibility Committee since March 2013. Defendant De Castro is a citizen of California.

31. Defendant Kenneth L. Salazar ("Salazar") has served as a Target director since July 2013. Defendant Salazar has also served as a member of Target's Corporate Responsibility Committee since November 2013. Defendant Salazar is a citizen of Colorado.

32. The defendants referenced above in ¶¶18-31 are collectively referred to herein as the "Individual Defendants." The defendants referenced in ¶¶18-20 above are referred to herein as the "Officer Defendants." The defendants referenced in ¶¶18 and 21-31 above are referred to herein as the "Director Defendants."

FIDUCIARY DUTIES OF THE INDIVIDUAL DEFENDANTS

33. The Individual Defendants have stringent fiduciary obligations to Target and its shareholders.

34. By reason of their positions as officers, directors, and/or fiduciaries of Target and because of their ability to control the business and corporate affairs of Target, the Individual Defendants owed Target and its shareholders fiduciary obligations of trust, loyalty, good faith, and due care, and were and are required to use their utmost ability to control and manage Target in a fair, just, honest, and equitable manner. The Individual Defendants were and are required to

act in furtherance of the best interests of Target and not in furtherance of their personal interest or benefit.

35. Each director and officer of the Company owes to Target and its shareholders the fiduciary duty to exercise good faith, loyalty, and diligence in the administration of the affairs of the Company and in the use and preservation of its property and assets, and the highest obligations of fair dealing. In addition, as officers and/or directors of a publicly held company, the Individual Defendants have a duty to promptly disseminate accurate and truthful information with regard to the Company's true forecasts and business prospects.

36. The Individual Defendants, because of their positions of control and authority as directors and/or officers of Target, were able to, and did, directly and/or indirectly, exercise control over the wrongful acts complained of herein, as well as the contents of the statements made publicly available and other actions taken in the aftermath of the data breach. Because of their advisory, executive, managerial, and directorial positions with Target, each of the Individual Defendants had access to adverse, non-public information about the financial condition, operations, and improper practices and representations of Target.

37. At all times relevant hereto, each of the Individual Defendants was the agent of each of the other Individual Defendants and of Target, and was at all times acting within the course and scope of such agency.

38. To discharge their duties, the officers and directors of Target were required to exercise reasonable and prudent supervision over the management, policies, practices, and controls of the financial affairs of the Company. By virtue of such duties, the officers and directors of Target were required to, among other things:

(a) refrain from acting upon material inside corporate information to benefit

themselves;

(b) ensure that the Company complied with its legal obligations and requirements, including acting only within the scope of its legal authority and disseminating truthful and accurate statements;

(c) conduct the affairs of the Company in an efficient, businesslike manner so as to make it possible to provide the highest quality performance of its business, to be in compliance with all applicable laws and rules, to avoid wasting the Company's assets, and to maximize the value of the Company's stock;

(d) devise and maintain a system of internal controls sufficient to ensure that the Company's customers' personal and financial information is protected;

(e) ensure that the Company timely and accurately informed customers regarding any breach of their personal and financial information;

(f) ensure that the Company was operated in a diligent, honest and prudent manner in compliance with all applicable laws, rules and regulations; and

(g) remain informed as to how Target conducted its operations, and, upon receipt of notice or information of imprudent or unsound conditions or practices, make reasonable inquiry in connection therewith, and take steps to correct such conditions or practices.

39. Each Individual Defendant, by virtue of his or her positions as a director and/or officer, owed to the Company and to its shareholders the fiduciary duties of loyalty, good faith, and the exercise of due care and diligence in the management and administration of the affairs of the Company, as well as in the use and preservation of its property and assets. The conduct of the Individual Defendants complained of herein involves a knowing and culpable violation of their obligations as directors and/or officers of Target, the absence of good faith on their part,

and a reckless disregard for their duties to the Company and its shareholders that the Individual Defendants were aware or should have been aware posed a risk of serious injury to the Company. The conduct of the Individual Defendants who were also officers and/or directors of the Company during the Relevant Period has been ratified by the remaining Individual Defendants who collectively comprised all of Target's Board during the Relevant Period.

40. The Individual Defendants breached their duties of loyalty and good faith by allowing the other Individual Defendants to cause, or by themselves causing, the Company to release false and misleading statements as detailed herein, by failing to properly oversee the Company's business and operations, and by failing to prevent the Individual Defendants from taking such illegal actions.

41. As members of the Board of the Company, the directors named herein as the Individual Defendants were themselves directly responsible for authorizing or permitting the authorization of, or failing to monitor, the practices which resulted in the worst data breach in American retail history and the dissemination of false and misleading statements regarding the scope of that breach as alleged herein. Each of the Individual Defendants had knowledge of, actively participated in, and approved of the wrongdoings alleged or abdicated his responsibilities with respect to these wrongdoings. The alleged acts of wrongdoing subjected the Company to unreasonable risk of loss, and have resulted in large losses to the Company.

42. By reason of their positions of control and authority as officers and/or directors of Target, the Individual Defendants were able to and did, directly or indirectly, cause the Company to engage in and/or permit the conduct complained of herein. The Individual Defendants also failed to prevent the other Individual Defendants from taking such illegal actions. As a result,

and in addition to the damage the Company has already incurred, Target has expended, and will continue to expend, significant sums of money.

43. Moreover, Target maintains a Business Conduct Guide (hereafter the "Guide"), which applies to "all Target board members and to team members at every level and every location of Target and its operating divisions and subsidiaries." The purpose of the Guide is to "to give [Target board members and employees] some tools to make decisions that reflect Target's commitment to exemplary corporate ethics and integrity." The Guide states in relevant part:

> **OUR COMMITMENT TO COMPLIANCE**
> Target has many teams dedicated to ensuring our business complies with all applicable laws and regulations. Complying with the requirements that govern our activities is vital to advancing our reputation. But the responsibility to drive compliance doesn't just belong to specific teams within the company. **It belongs to you!** In fact, every team member, in every part of the organization, plays a role in compliance: from the business partner at headquarters making sure that our prices are accurate, to the warehousing team member at the distribution center staying current on the training requirements for her job, the pharmacy technician protecting guests' medical information, or the ETL removing expired products from our shelves. All of these team members help Target comply with its regulatory obligations.
>
> Best practices, policies, and procedures are some of the tools designed to enable Target to achieve its commitment to compliance. You are responsible for understanding these tools and knowing how and when to use them. If you're unsure about what's expected of you, talk with your supervisor to learn what to do. We take compliance very seriously and no one should dismiss the responsibility to meet these requirements. This guide is about the integrity and high ethical standards that are part of Target's culture: the cornerstone of these attributes is our team members' dedication to and ownership of compliance.
>
> ***
>
> *6 Protecting Target's Assets*
> **USE AS DIRECTED**
> Target's assets—no matter whether they're merchandise, vendor samples, corporate credit cards, cash or information—are intended to be used for the benefit of the company. Target has accounting, reporting and internal controls and

teams in place to detect theft, fraud or misuse of company assets. When theft does occur, we investigate and resolve each incident quickly.

It's a pretty good bet that you already know your role in protecting Target's assets. If you don't, read the company's policies. If you see somebody stealing, or if you become aware of misuse of company assets, **alert your supervisor, Assets Protection or the Employee Relations and Integrity Hotline.**

7 Record Retention

TO KEEP OR NOT TO KEEP?

Many of us collect a lot of information in the course of doing our jobs—e-mails, memos, spreadsheets, contracts, proposals, project plans…the list goes on and the documents stack up. If you don't know how long you're supposed to keep that information, you risk keeping it too long or getting rid of it too soon. Cleaning out your files might result in discarding information that we need to keep, while keeping documents too long can result in confusion and an overstuffed electronic archive.

We have an obligation to ensure that our records are kept for the required amount of time. **Talk to your supervisor** to be sure that you understand the legal requirements and company expectations for keeping documents for which you're responsible, and the right way to dispose of documents we're no longer required to keep. You can also **contact Records Management** for a copy of our corporate records retention schedule.

***

9 Advertising

SAY IT PLAIN

Guests are loyal to Target because they trust us to bring them high-quality merchandise at a good value, and to be a partner in building healthy communities. We've built that trust over decades, but we can damage it in an instant if we tell our guests something that turns out not to be true.

That's why our goal is clarity and accuracy in every advertisement we run. The claims made have to be true and supported; prices have to be accurate; we strive to have advertised merchandise available for guests to buy; and if the merchandise doesn't live up to guest expectations, we need to abide by our return policy. It's all about maintaining Target's brand and reputation.

***

12 Credit and Financial Services

THE RULES ARE THE RULES

We offer credit to our guests through the Target® VISA® card, the REDcard® (both issued by Target National Bank), and the Target Business Card® (issued by

Target Bank). Other Target financial products include the Target GiftCard®, the Target Debit CardTM and the Target® Visa® Gift Card.

The state and federal laws and regulations that apply to consumer financial products and services run to thousands of pages. They govern everything from how we advertise our financial products and how we disclose product terms to how we manage cardholders' accounts and collect on past-due balances. There are even laws restricting how Target GiftCards can be displayed in our stores. If you're involved in creating, marketing or managing any of our financial products, you're responsible for following the designated procedures to meet our compliance obligations.

***

20 Financial Integrity and Reporting
FOR THE RECORD
Target keeps records that reflect our financial statements and transactions with complete accuracy, and is committed to providing full, fair, accurate, timely and understandable disclosure in its external communications. The U.S. Securities and Exchange Commission and other governing bodies have strict rules about the accuracy of our financial statements and disclosures and about the strength of our internal controls over financial reporting. The Target Assurance team checks our internal controls periodically, and an outside auditor also checks the accuracy of our financial statements and disclosures. If anyone ever asks you to falsify a financial record, **tell your supervisor, call the Employee Relations and Integrity Hotline or e-mail Integrity@Target.com right away**—and remember that Target prohibits retaliation against any team member who makes a report in good faith.

44. In addition to these sections of the Guide that describe basic duties tangential to protecting customer personal and financial information, the Guide also contains a section that directly applies to the Individual Defendants' duties with regard to the personal and financial information of customers. That section of the Guide reads as follows:

18 Information Protection and Privacy
PAUSE, PROTECT, PROCEED
When guests share their personal information with us—like their names and addresses, credit card numbers and Social Security numbers—they expect Target to keep that information safe. If we break that trust, we'll damage Target's reputation and our relationship with guests. If someone asks you to share information, verify that they are who they say they are and that they're authorized to have the information they want.

No matter which area of Target you work in, you have access to information that could impact the reputation or financial well-being of Target, our guests and our team members if it falls into the wrong hands. Whether you work with protected health information, team-member information or business information such as price points, merchandise allocation, non-public financial information or company initiatives, you're entrusted to ensure that only people with a business need have access to the information you create, share and store.

All Target team members are expected to know and follow our Information Protection Policy. The policy outlines how information is classified at Target and how you should protect the information you work with throughout its life cycle. Target is subject to laws that require us to protect certain types of information and specify how that information should be protected.

When you're working with any kind of information, you should:
Pause to understand its classification. Target classifies information according to its level of sensitivity.
• **Secure Handling Required (SHR)** requires the highest levels of protection
• **Confidential** requires a high level of protection
• **Internal** can be shared with Target team members, contractors and authorized business partners
• **Public** can only be classified as such by only team members authorized to approve the release of information outside of Target

Protect information as required.
• Store data in a location accessible only to those who have a business need to know.
• Share data only with team members or vendors who need the information to do their jobs.
• Before sharing data with a vendor, ensure that the vendor has completed any necessary risk assessments and signed a confidentiality agreement with Target.
• Send data via secure methods according to its classification.
• Consult retention guides and schedules to know how long data needs to be stored and when it should be destroyed.
• Ensure that information is disposed of properly and according to its classification.

Proceed wisely according to the classification of the information you are using and the protection it requires.

> Ask yourself: Is it okay for me to collect or share this information? Can the other team members or vendors I'm working with do their jobs without this information?

Want more detail? **Read the Target Information Protection Policy or e-mail Integrity@Target.com**

> Getting personal? Get the fine print right. *When the Target Marketing team came up with the idea for a new campaign that would ask guests to register online and provide some personal information, they wanted to reassure guests—so they included language that said Target would use the collected information only for that specific campaign. But when Marketing checked with the Target Law department about how the language should read, they decided that definitive statements like the one Marketing proposed could conflict with Target's legal obligations, published privacy policies, or internal policies and practices. Target's Law team helped Marketing rewrite the language to make sure it was accurate and consistent with our policies.*
>
> The ways in which Target collects, uses and shares guests' and team members' personal information all fall under the umbrella of "data privacy." Not only do we comply with applicable laws and regulations about how we handle guests' financial information and guests' and team members' health information, we've also created privacy policies that cover specific types of information (e.g., bank data and medical records) as well as a comprehensive privacy policy that covers collection, use and sharing of guest information. Some of our policies give guests and team members options for how their information will be used or shared.
>
> If your job involves guests' or team members' personal information, it's important for you to **be aware of these policies and know how they apply to your work.** And it's equally important to consider these policies if we want to share guest or team-member information not just with third parties outside of Target, but also when we share information between Target affiliates like Target Stores and Target National Bank.
>
> > Ask yourself: Is there a privacy policy that applies to the information that I want to use or share?
>
> Want more detail? **E-mail Integrity@Target.com**.

45. Similarly, the members of the Audit Committee—Defendants Austin, Minnick, Mulcahy, and Rice—are governed by the rules set forth in the Audit Committee Position Description (hereafter the "Audit Committee Charter"). The Audit Committee Charter states that one function of the Audit Committee is "[t]o assist the Board of Directors in monitoring the integrity of the Corporation's financial statements, the independence, qualifications and performance of the Corporation's independent auditor, the performance of the Corporation's

internal audit function, the Corporation's compliance with legal and regulatory requirements and to approve the Committee's report for inclusion in the Corporation's Proxy Statement."

46. To that end, the Audit Committee's primary responsibilities and duties include, among other things, to:

> **RESPONSIBILITIES:**
> **A. Accounting and Reporting**
> **1. Review of Press Releases and Other Information.** Discuss the Corporation's earnings press releases (including the use of "pro forma" or "adjusted" non-GAAP information), as well as financial information and earnings guidance provided to analysts and ratings agencies (discussion may be done generally and need not occur prior to each release).
>
> ***
>
> **4. Internal Controls - General.** Receive information from management about any significant deficiencies or material weaknesses in the design or operation of internal controls that could adversely affect the Corporation's ability to record, process, summarize and report financial data and any fraud, whether or not material, that involves management or other employees who have a significant role in the Corporation's internal controls. The Committee shall also review the independent auditor's letter reporting the status of internal controls and other matters the independent auditor considers appropriate and obtain and review management's response and corrective action plan.
>
> ***
>
> **6. General Oversight.** Discuss with management and the independent auditor significant financial reporting issues and judgments made in connection with the preparation of the Corporation's financial statements, including any significant changes in the Corporation's selection or application of accounting principles and any critical accounting estimates made in the course of preparing the financial statements.
>
> ***
>
> **D. Compliance Oversight**
> **1. General.** Oversee the Corporation's ethics and compliance programs, including its Business Conduct Guide, and receive periodic reports on such programs from appropriate members of management.
>
> **2. Investigations.** Conduct any investigation that the Committee deems appropriate, with full access to all of the Corporation's records, facilities,

personnel and outside advisors, and retain outside counsel, auditors and other consultants to advise the Committee for that purpose or others. The Corporation shall provide appropriate funding, as determined by the Committee, for payment of any resource engaged for this purpose and for all other administrative expenses necessary for the Committee to carry out its duties.

3. Accounting and Auditing Complaints. Establish procedures for the receipt, retention and treatment of complaints received by the Corporation regarding accounting, internal accounting controls or audit matters, and the confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters.

4. Legal Matters. Review periodic reports of the General Counsel on litigation and other legal matters that may have a material impact on the financial statements or the Corporation's internal controls.

47. In derogation of these duties, Defendants Austin, Minnick, Mulcahy, and Rice, the members of the Audit Committee, failed to adequately monitor the Company's press releases and compliance with data protection laws and regulations.

FACTUAL ALLEGATIONS

Background

48. As the nation's second largest general merchandise retailer, Target operates 1,797 stores in the United States. The Company also expanded into Canada in March 2013, where it operates 124 stores. The Company operates through three reportable segments: the U.S. Retail segment, the U.S. Credit Card segment, and the Canadian segment. The U.S. Retail segment includes all of the Company's physical stores, online, and catalog stores in the United States; the Credit Card segment operates Target's branded proprietary credit cards; and the Canadian segment operates the Company's March 2013 foray into Canadian market.

49. Historically, Target has used its power as the number two retailer in the United States to lobby against new technologies that would enhance the security of credit and debit card transactions. Many stores in Europe and Canada use chip-based credit cards that are much harder to replicate than normal credit cards. In 2004, Target moved against the new cards out of

fear that they would slow checkout speeds. Advocates had hoped that Target would adopt the program prior to 2004, which would have likely led to widespread adoption in the U.S. Because Target opted against the enhanced security program, the U.S. is now purposefully targeted for criminal cyber-attacks because of its position as one of the last remaining developed counties that does not take advantage of the more secure technology.

50. Target maintains a "Privacy Policy," which explains that the Company routinely collects personal information from its customers including a customer's name, mailing address, e-mail address, phone number, driver's license number, and credit/debit card number. In addition, when customers use their debit cards to make a purchase at Target, just as when they make a purchase using a debit card anywhere, they are required to enter the PIN associated with their bank account. In the "Privacy Policy," Target promises its customers that it will, among other things:

> …maintain administrative, technical and physical safeguards to protect your personal information. When we collect or transmit sensitive information such as a credit or debit card number, we use industry standard methods to protect that information.

51. Blatantly breaking its promise and violating its duties to protect its customers' sensitive personal and financial information, the Individual Defendants caused Target to allow the sensitive and private information of over one hundred ten million customers to be compromised. Target's widespread failure to protect its customers' critical personal and financial information exposed victims to identity theft and has significantly damaged Target.

52. Armed with a customer's personal and financial information, identity thieves can easily encode the victim's account information onto a blank card with a magnetic strip creating a counterfeit card that can be used to make fraudulent purchases. With the addition of a victim's

PIN, a thief can use the counterfeit card to withdraw money directly from that person's bank account at any ATM machine (or automated teller machine) in the world.

53. Identity thieves can further exploit their victims by using personal information in a vast varieties of ways, including to open new credit, bank, and utility accounts, get cash advances, make large purchases, receive medical treatment on the victim's health insurance, and obtain to a driver's license or passport. Once an identity has been stolen, reporting, identifying, monitoring, and repairing the victim's credit is a stressful, time-consuming, expensive, and cumbersome process. On top of the frustration of having to identify and close affected accounts and correct information in credit reports, the victims of identity theft often incur costs associated with defending themselves against collection actions brought by creditors. Victims also suffer damage to their credit score and an enhanced burden when seeking new credit. Moreover, victims of identity theft must continue to monitor their credit reports for several years because fraudulent acts may not take place several years, yet still remain possible. Early estimates show that a mass breach of this nature will likely cost approximately $5.10 per card that was exposed. For a breach of this magnitude, the total costs may very well approach $561 million to Target.

54. The significance of protecting personal and financial information has pushed the federal government to enact of copious privacy-related laws aimed toward protecting consumer information and disclosure requirements. This legislation includes: (i) the Gramm-Leach-Bliley Act (the Financial Services Modernization Act of 1999); (ii) the Fair Credit Reporting Act; (iii) the Fair and Accurate Credit Transactions Act; (iv) the Federal Trade Commission Act; (v) the Health Insurance Portability and Accountability Act; (vi) the Health Information Technology for Economic and Clinical Health Act; (vii) the Driver's Privacy Protection Act; (viii) the E-Government Act of 2002; (ix) the Social Security Act Amendments of 1990; (x) the Privacy Act

of 1974; and (xi) the Federal Information Security Management Act of 2002. The federal government also maintains the newly created Consumer Financial Protection Bureau, which was established as an independent federal agency holding the primary responsibility for regulating consumer protection with regard to financial products and services in the United States.

55. Identity theft perpetrated over the internet as a cyber-attack is becoming more and more common in the digital age. A series of recent major cyber-attacks striking American corporations has prompted warnings from federal officials. In fact, as recently as May 2013 ICS-Cert, a division of the Department of Homeland Security that monitors attacks on computer systems that run industrial processes, issued a warning that the government was "highly concerned about hostility against critical infrastructure organizations."

56. The Individual Defendants were fully aware of the risk of a potential data breach. On August 27, 2007, Dr. Neal Krawetz, a data security expert working for Hacker Factor Solutions, issued a paper titled "Point-of-Sale Vulnerabilities." The paper warned Target and its peer major national retailers about the possibility of a point-of-sale data breach. The paper laid out the exact areas of vulnerability and even used Target as an example of the potential ramifications of a point-of-sale data breach at a major retailer. Further, Dr. Krawetz's paper estimated that as many as fifty-eight million card accounts could be compromised if Target's point-of-sale system was compromised. This was a widely-read paper and the Individual Defendants were undoubtedly aware of its findings.

57. The Individual Defendants have even acknowledged the risk of a data breach, yet failed to take any action to prevent that risk from coming to fruition. In its 2012 Form 10-K filed with the SEC on March 20, 2013, Target included a risk disclosure stating that the Company was fully aware of the consequences of failing to keep customers' data secure and that the Company

could be subject to costly government enforcement actions and private litigation. The relevant portion of the Form 10-K read as follows:

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

The Data Breach

58. The data breach that took place in November and December 2013 compromised one hundred ten million Target customers' personal and financial data. Within days of the breach, millions of affected customers' financial and personal information was being sold on the black-market.

59. The first news of the data breach did not come from Target, but was broken by KrebsOnSecurity.com on December 18, 2013. The website dedicated to reporting cybercrime, published an article indicating the occurrence of a massive data breach at Target stores. According to the article, Target was investigating the possible theft of millions of customer credit card and debit card records beginning November 27, 2013, and extending as far as December 15, 2013. The breach was said to have occurred when thieves accessed the Company's customers' personal and financial data by penetrating Target's point-of-sale system.

The Individual Defendants' False Statements to Customers

60. Target's customers were entitled to have the information they entrusted to Target protected to the greatest extent possible. And in the unlikely event that the data was breached, Target's customers were entitled to immediate, full, and accurate notification of the data breach to help them mitigate the harm and avoid additional instances of fraud. Conversely, the

Individual Defendants, failed to take the appropriate steps to cause the Company to notify customers that their sensitive information had been obtained by nefarious individuals for nefarious purposes. In so doing, the Individual Defendants served to aggravate the damage to affected customers and the Company.

61. After numerous third-party sources spread the news of the data breach across the news media for twenty-four hours, Target finally public acknowledged that its security systems had been compromised and its customers' trust had been betrayed. On December 19, 2013, over three weeks after the data breach began and four days after it had been contained, Target finally admitted the breach to the public. The Company issued a brief statement in which it confirmed that it had been aware of unauthorized access to certain customers' credit and debit card data at the Company's U.S. stores. The statement read as follows:

> **Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores**
>
> Issue has been identified and resolved
>
> MINNEAPOLIS — December 19, 2013
>
> Target today confirmed it is aware of unauthorized access to payment card data that may have impacted certain guests making credit and debit card purchases in its U.S. stores. Target is working closely with law enforcement and financial institutions, and has identified and resolved the issue.
>
> "Target's first priority is preserving the trust of our guests and we have moved swiftly to address this issue, so guests can shop with confidence. We regret any inconvenience this may cause," said Gregg Steinhafel, chairman, president and chief executive officer, Target. "We take this matter very seriously and are working with law enforcement to bring those responsible to justice."
>
> Approximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013. Target alerted authorities and financial institutions immediately after it was made aware of the unauthorized access, and is putting all appropriate resources behind these efforts. Among other actions, Target is partnering with a leading third-party forensics firm to conduct a thorough investigation of the incident.

62. The Company's statement aims to minimize the impact of the breach, stating that "[a]pproximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013." Later, this initial statement would prove to be untrue.

63. In a separate statement issued that same day by defendant Steinhafel, Target explained more of the details of exactly what information was compromised. Defendant Steinhafel's December 19, 2013 statement stated that the data breach "included customer name, credit or debit card number, and the card's expiration date and CVV [card verification value, the three numbers on the reverse side of Visa and MasterCards or the four smaller numbers on the front side of American Express cards]." Defendant Steinhafel's statement restated the claim that "[t]he unauthorized access may impact guests who made credit or debit card purchases in our U.S. stores from Nov. 27 to Dec. 15, 2013."

64. The next day. December 20, 2013, in a publicity stunt attempting to contain and minimize the public perception of the impact of the data breach, defendant Steinhafel declared to "have worked swiftly to resolve the incident" and concluded that, "there is no indication that PIN numbers have been compromised on affected bank issued PIN debit cards or Target debit cards." Defendant Steinhafel further assured frazzled customers that "[s]omeone cannot visit an ATM with a fraudulent debit card and withdraw cash." That same day, defendant Steinhafel issued a press release on behalf of Target announcing that "the issue has been identified and eliminated" and that the Company would provide free credit monitoring services to affected customers. In an effort to restore confidence in the Company and keep the news of the breach from destroying the last few days of the 2013 holiday shopping season, Target offered to extend its employees' discount of 10% to all customers who shopped in Target stores on the weekend of December 21 and 22, 2013.

65. From the moment they were informed of the breach, the Individual Defendants tried to minimize reports regarding the extent of the breach and to protect Target sales during the 2013 holiday shopping season, in spite of the fact that such efforts would only serve to further erode customer confidence when the truth was finally revealed and cause greater damage to Target's reputation, brand, and goodwill.

66. As expected, despite Target's attempts to dispel customers' concerns, news once again began to emerge that credit and debit card information stolen from Target was appearing for sale online. According to several sources, customer account information stolen from Target was being sold on the black market in batches of one million cards and fraudulent purchase activity had begun being reported by issuing banks.

67. With each passing day, independent sources began to find and reveal more of the true scope of the breach. On December 23, 2013, Target acknowledged that the Secret Service and the DOJ decided to participate in the investigation into the breach. Additionally, the Company stated that it had spoken with the attorneys general for Massachusetts, New York, Connecticut, and South Dakota concerning the breach. Those attorneys general have now been joined by counterparts in Illinois, California, Minnesota, and several other states to investigate the breach.

68. The following day, news came out that, despite prior statements by Target to the contrary, encrypted PIN data had been stolen during the original breach and that those codes could be used by thieves to make fraudulent withdrawals from the victims' bank accounts. In response to these allegations, Target continued to deny that any of its customers' PIN data had been compromised. Defendant Steinhafel maintained that "[t]here is no indication that PIN

numbers have been compromised on affected bank issued PIN debit cards or Target debit cards" and that "[s]omeone cannot visit an ATM with a fraudulent debit card and withdraw cash."

The True Scope of the Breach is Finally Revealed

69. Then, on December 27, 2013, two days after Christmas and the conclusion of the 2013 holiday shopping season, Target finally admitted that customers' PIN data had been compromised in the breach. On January 10, 2014, Target disclosed that 70 million customers' personal information may also have been affected by the data breach, bringing the total of possible victims up to over one hundred ten million Target customers. Additionally, this new swath of victims did not consist of only those customers who had made purchases at physical Target stores between November 27 and December 15, 2013, it included all Target customers online and in-store spanning as far back as ten years.

The Individual Defendants Failed to Implement Appropriate Security Measures

70. On the Company's website Target recognizes that its customers' personal and financial information is highly sensitive and must be protected. The Company maintains a Privacy Policy, that gives the following promise regarding personal information:

> We maintain administrative, technical and physical safeguards to protect your personal information. When we collect or transmit sensitive information such as a credit or debit card number, we use industry standard methods to protect that information.

71. There are currently at least nineteen class action lawsuits being brought by Target's customers against the Company for the data breach. In defending against those suits, Target will likely try to prove that it had been fully compliant with industry standards and therefore had done all it could to protect against the breach. The most prominent of these industry standards is the PCI Data Security Standard ("PCI"). The PCI is an industry standard

for large retail institutions that accept credit card and debit card transactions, but it is far less than it is cracked up to be. The standard consists of twelve general requirements including:

1. Install and maintain a firewall configuration to protect cardholder data;
2. Do not use vendor-supplied defaults for system passwords and other security parameters;
3. Protect stored cardholder data;
4. Encrypt transmission of cardholder data across public networks;
5. Use and regularly update anti-virus software or programs;
6. Develop and maintain secure systems and applications;
7. Restrict access to cardholder data by business need to know;
8. Assign a unique ID to each person with computer access;
9. Restrict physical access to cardholder data;
10. Track and monitor all access to network resources and cardholder data;
11. Regularly test security systems and processes; and
12. Maintain a policy that addresses information security for all personnel.

72. Even if Target is found to be in compliance with PCI, there is growing concern that the standard is not adequate to protect consumers. The system has been criticized for fostering complacency among merchants that meet the standards and offering the merchants a means of avoiding blame.

73. Nevertheless, on December 23, 2013, USA Today reported that Target was likely not even in compliance with the low standard of PCI. The article stated:

> Target's massive databreach took place just a few weeks before a set of payment card industry standards - known as PCI DSS 3.0 - were scheduled to go into effect. CyberTruth asked Nick Aceto, technology director at software vendor CardConnect, to supply some clarity.
>
> CyberTruth: What does this latest databreach tell us about the efficacy of PCI?
>
> Aceto: We can't say definitely that this breach is a failure of Target's PCI compliance, but based on what Target has said, it's very hard to believe that they were even PCI 2.0 compliant at the time of the breach.
>
> A reason for thinking this is that the attack, involving an enormous amount of data, went on essentially unnoticed for 18 days. How were they not watching the network?
>
> One of the PCI DSS requirements is that you monitor your logs and firewalls every day, looking for unusual activity. This monitoring involves file integrity

> checks and changes to critical systems files. What's more - the chapter 6 software development life cycle requires the secure distribution and verification of payment applications.
>
> Unusual activity isn't always abnormal, but the point of PCI is to monitor and verify that all activity is normal, while not letting distractions - like busy shopping days Black Friday and Cyber Monday, on which the breach occurred - detract from the monitoring effort.

74. The Individual Defendants knew or should have known that the Company had failed to meet industry standards with its security systems and left its technologies unreasonably vulnerable rendering its customers a target of attacks by nefarious third-parties. The Individual Defendants, however, failed to take corrective measures to update Target's systems and technologies. Target's deficiencies included the failure to maintain adequate backups and/or redundant systems; failure to encrypt data and/or establish adequate firewalls to handle a server intrusion contingency; and failure to provide prompt and adequate warnings of security breaches.

The Aftermath of the Breach and its Lasting Effect

75. Once the full scope of the data breach became clear, so did its historical significance. A January 11, 2014 NBC News article quoting Ken Stasiak, the CEO of cyber-security company SecureState, called Target's breach "***the worst breach in history***." Mr. Stasiak went on to say, "It's 2014. We expect retailers of this magnitude to have better security, weigh their risks and spend the resources necessary to secure their data." Empirically, Target's breach is the worst in history because it concerned the data of over one hundred ten million customers, far outreaching the previous holder of the title, TJX Companies, Inc. (parent of TJMaxx, Marshall's, and HomeGoods) with a breach of forty-five million customers' information in 2007.

76. Target itself has suffered considerable damage from breach itself and the bungling of its aftermath. In response to events described above, market analysts such as Cowen and Co. have lowered ratings on Target and trimmed price expectations. Cowen had formerly targeted

Target's price for $66 per share, but on January 21 reduced that number to $47 per share. Target shares were trading above $63.50 on December 18, 2013 before the news of the data breach and have fallen over 10.5% to $57.60.

77. On top of the loss in market capitalization, the economic impact of the breach has been felt throughout Target. The Company announced on January 22, 2014 that it was cutting health coverage for part-time workers as well as laying-off 475 workers and eliminating 700 open positions.

78. Public backlash from the breach is also far from over. While the Individual Defendants have tried to control the public relations nightmare of the breach on their own terms, federal legislators are now stepping in to further shame the Company. Defendant Mulligan has been called to appear before the U.S. Senate Judiciary Committee on February 4. This will be the first time that Target will be forced to answer questions about the worst breach in history. Preparation for this hearing and whatever action comes out of it, will likely cost the Company great sums of money in addition to that already being spent to quell the financial damage caused by the breach.

DERIVATIVE AND DEMAND FUTILITY ALLEGATIONS

79. Plaintiff brings this action derivatively in the right and for the benefit of Target to redress injuries suffered, and to be suffered, by Target as a direct result of the Individual Defendants' breaches of fiduciary duty.

80. Plaintiff will adequately and fairly represent the interests of the Company and its shareholders in enforcing and prosecuting its rights.

81. Target is named as a nominal defendant in this case solely in a derivative capacity. This is not a collusive action to confer jurisdiction on this Court that it would not otherwise have. Plaintiff is and was a shareholder of Target at the time of the transgressions

complained of. Prosecution of this action, independent of the current Board of Directors, is in the best interests of the Company.

82. The wrongful acts complained of herein subject, and will continue to subject, Target to continuing harm because the adverse consequences of the actions are still in effect and ongoing.

83. The wrongful acts complained of herein were unlawfully concealed from Target's shareholders.

84. Throughout the Relevant Period, the Individual Defendants violated multiple corporate governance principles, thus representing evidence of the Individual Defendants' breaches of fiduciary duties. The course of action included failing to maintain appropriate data security systems and concealing the truth about the breach from the public, and caused the Individual Defendants to breach the following corporate principles, among others:

a. protect customers' personal and financial information in accordance with the Privacy Policy, the Guide, and industry best practices;

b. maintain a system of internal controls that will provide reasonable assurances to management that material information about the Company is made known to management, particularly information being conveyed by the Company that concerns the public trust; and

c. comply with all local and federal laws and regulations.

85. As a result of the facts set forth herein, Plaintiff has not made any demand on the Target Board to institute this action since such demand would be a futile and useless act because the Board is incapable of making an independent and disinterested decision to institute and vigorously prosecute this action. The wrongful acts complained of herein show a wholesale

abandonment by the Individual Defendants of their fiduciary duties of due care, oversight, and loyalty. Such abandonment includes, but is not limited to the following:

a. Allowing for materially inadequate controls over the Company's policies with respect to cyber-security and the protection of sensitive customer information;

b. Allowing the Company to make false statements concerning the data breach and to withhold the breach from the affected customers; and

c. Failing to adequately remedy the data breach in the fashion expected of the second largest retailer in the United States.

86. At the time of filing, the Board consisted of twelve individuals: Defendants Steinhafel, Johnson, Trujillo, Mulcahy, Austin, Darden, Minnick, Rice, Stumpf, Baker, De Castro, and Salazar. Plaintiff did not made any demand on the Board to institute this action because such a demand would be a futile, wasteful, and useless act, particularly for the following reasons:

a. As a result of their access to and review of internal corporate documents, conversations and connections with other corporate officers, employees and directors; and attendance at management and the Board meetings during the Relevant Period, each of the Director Defendants knew, or were reckless in not knowing, that the Company was obscenely vulnerable to a cyber-security attack upon customers personal and financial information that would subject the Company to hundreds of millions of dollars in liability, yet failed to take any meaningful action to correct these problems and foster compliance with applicable laws and regulations; and

b. The Director Defendants were particularly aware of the industry standards for secure transactions and new technologies that could have enhanced security and chose not to implement further security measures and to lobby against the widespread adoption of new technology.

87. Defendants Steinhafel, Johnson, Trujillo, Mulcahy, Austin, Darden, Minnick, Rice, Stumpf, Baker, De Castro, and Salazar, the Company's entire current Board, caused the Company to withhold and then disseminate improper, materially false and misleading public statements concerning, among other things, the true nature and extent of the data breach. Customers were entitled to adequate and prompt notification about the data breach to help them mitigate the harm and avoid additional instances of fraud. The Individual Defendants, however, failed to take reasonable steps to have the Company notify consumers that their information had been compromised. The Company's public disclosures concerning the data breach were improper because: (i) they were untimely and only released after third-party organizations began spreading the news; (ii) they understated the scope of the affected victims by seventy million people; (iii) they diminished the severity of the harm to customers by failing to disclose that PINs were compromised, (iv) withheld the scope of the personal data that was compromised, and (v) allowed for a secondary breach to occur in the aftermath of the initial breach in the form of fraudulent credit monitoring emails. Each member of the Board knew or should have known that the improper statements did not timely, fairly, accurately, or truthfully convey the scope of the data breach. In addition, when deciding whether to approve statements to be publicly disseminated, each member of the Board was bound by the duty of care and the duties set forth in the Guide to inform himself or herself of all reasonably-available material information. Information concerning the nature and extent of the data breach was both reasonably available

and material to members of the Board. Defendants Steinhafel, Johnson, Trujillo, Mulcahy, Austin, Darden, Minnick, Rice, Stumpf, Baker, De Castro, and Salazar's conduct can in no way be considered a valid exercise of business judgment. Accordingly, demand on the Board is excused as futile.

88. A majority of the Board is incapable of disinterestedly and independently considering a demand to commence and vigorously prosecute this action for the following reasons:

a. Defendants Steinhafel, Johnson, Trujillo, Mulcahy, Austin, Darden, Minnick, Rice, Stumpf, Baker, De Castro, and Salazar, are substantially likely to be held liable for breaching their fiduciary duties, gross mismanagement, abuse of control, and by maintaining inadequate internal control of information privacy and cyber-security as complained of herein.

b. Further, Defendants Steinhafel, Johnson, Trujillo, Mulcahy, Austin, Darden, Minnick, Rice, Stumpf, Baker, De Castro, and Salazar face a substantial likelihood of liability due to their failure to provide adequate and prompt notice to consumers and because they conveyed a false sense of security to customers affected by the data breach. Defendants Steinhafel, Johnson, Trujillo, Mulcahy, Austin, Darden, Minnick, Rice, Stumpf, Baker, De Castro, and Salazar breached their duty of loyalty by causing the Company to disseminate the improper public statements discussed herein. Accordingly, all the Board members face a substantial likelihood of liability, rendering demand upon them futile.

c. Defendant Steinhafel is both Target's CEO and President. Defendant Steinhafel is not disinterested because it is very likely that he will be held liable in any action brought on behalf of the corporation for his alleged wrongdoing. In fiscal year 2012, Defendant Steinhafel

received $20,647,464 in compensation from Target. Due to his excessive compensation and position as an insider in the Company, he is entrenched in the Company.

d. Defendants Johnson, Trujillo, Mulcahy, Austin, Darden, Minnick, Rice, and Stumpf each received over $250,000 in compensation for their service as directors in 2012. Due to their significant director compensation, Defendants Johnson, Trujillo, Mulcahy, Austin, Darden, Minnick, Rice, and Stumpf are disabled from impartially considering a demand to prosecute the claims herein.

e. Several of the Director Defendants have served long tenures as directors with the Company and cannot objectively appraise whether to pursue an action upon themselves and their colleagues. Defendant Johnson has served as a director since 1996. Defendant Trujillo has served as a director since 1994. Defendant Mulcahy has served as a director since 1997. Defendant Austin has served as a director since 2002. Defendant Darden has served as a director since 2003. Defendant Minnick has served as a director since 2005. Due to their long tenure and the close business relationships built up over nine-plus years of common service on the Target Board, defendants Johnson, Trujillo, Mulcahy, Austin, and Minnick are disabled from impartially and independently considering a demand to sue their fellow directors with whom they have established significant professional ties.

f. Defendants Austin, Minnick, Mulcahy, and Rice all served as members of the Audit Committee during the Relevant Period. Defendant Austin was and continues to be the Chairman of the Audit Committee. According to the Audit Committee Charter, Defendants Austin, Minnick, Mulcahy, and Rice have the specific duty to oversee all material aspects to the Company's reporting, control, and audit functions. Because they breached that duty, there is a high likelihood that they will be held personally liable in any litigation brought on behalf of the

Company. It is for this reason, among others, that the members of the Audit Committee are not disinterested and cannot reasonably decide whether to bring litigation against themselves on behalf of the Company.

89. During the Relevant Period the Individual Defendants caused or allowed the Company to fail to maintain proper internal controls over their security and privacy systems and to issue false and misleading statements when those systems were breached. The Individual Defendants' misconduct has severely damaged, and will continue to severely damage, the Company. Further, and more importantly, Target's reputation, goodwill, brand trust, and positive brand recognition have been tainted by the misconduct described herein.

90. As detailed above, the Board members were directly involved in the misconduct challenged in this action, by virtue of their respective positions on the Board and its Committees, and completely abdicated their responsibility to oversee the Company's operations, causing the Company to engage in illegal and/or improper conduct regarding cyber-security and the public statements and surrounding the breach, destroying in their wake, much of the Company's shareholder value. The Individual Defendants' conduct lacked any legitimate business purpose and was not a product of a valid exercise of business judgment. As such, demand is excused as futile.

91. The Individual Defendants' conduct described herein and summarized above demonstrates a pattern of misconduct that could not have been the product of legitimate business judgment as it was based on intentional, reckless, and disloyal misconduct. Thus, none of the Individual Defendants, who constitute the entire current Board of the Company, can claim exculpation from their violations of duty pursuant to the Company's Articles of Incorporation. As a majority of the Individual Defendants face a substantial likelihood of liability, they are self-

interested in the transactions challenged herein and cannot be presumed to be capable of exercising independent and disinterested judgment about whether to pursue this action on behalf of the shareholders of the Company. Accordingly, demand is excused as being futile.

92. Furthermore, the Target Board is still dominated and controlled by the exact same wrongdoers who continue to obscure their own misconduct, and will not take action to protect the interests of Target or its shareholders. The present Board has refused, and will continue to refuse, to institute this action for the foregoing and following reasons:

a. The acts complained of herein constitute violations of fiduciary duties owed by the Board of Directors and these acts are incapable of ratification;

b. Certain of the known principal wrongdoers and beneficiaries of the wrongdoing complained of herein are in a position to, and do, dominate and control the Board of Directors. Thus, the Board could not exercise independent objective judgment in deciding whether to bring or vigorously prosecute this action;

c. The acts complained of herein are illegal and improper and thus are acts incapable of ratification;

d. In order to bring this action for breach of fiduciary duty, the members of the Board of Directors would have been required to sue themselves and/or their fellow directors and allies in the top ranks of the Company, who have personal relationships and with whom they have entangling financial alliances, interests, and dependencies, which they would not do. They therefore would not be able to vigorously prosecute any such action; and

e. The members of the Target Board, including each of the Defendants herein, receive substantial salaries, bonuses, payments, benefits, and other emoluments by virtue of their membership on the Board and their control of Target. They have thus benefited from the wrongs herein alleged and have engaged therein to preserve their positions of control and the perquisites thereof, and are incapable of exercising independent objective judgment in deciding whether to bring this action. The Board members also have close personal or business ties with each other and are, consequently, interested parties and cannot in good faith exercise independent business judgment to determine whether to bring this action against themselves.

93. Moreover, each of the Individual Defendants, as an officer and/or director of Target, had intimate knowledge of all major operations of the Company, and yet participated in maintenance of inadequate cyber-security controls and the dissemination of material misstatements about the scope of the breach. Thus, the Individual Defendants all have a personal interest in concealing any blame for Target's internal controls problems, and shifting the blame away from themselves for consciously disregarding fiduciary duties. An investigation or inquiry that spread blame higher up the corporate ladder—to the Individual Defendants, as officers and/or directors—would not be in the personal interest of the Individual Defendants. The result of such an inquiry would require them to return valuable but unearned compensation to the Company.

94. In addition, all Individual Defendants face a sufficiently substantial likelihood of liability, and thus, there is a reasonable doubt as to each of their disinterestedness in deciding whether pursuing legal action would be in the Company's best interest.

95. Further, any suit by the current directors of Target to remedy these wrongs would expose Target to liability in the numerous pending consumer class actions lawsuits. There are currently no less than nineteen consumer class actions filed against the Company as a result of the data breach. These class actions allege various claims, including, but not limited to, negligence, breach of contract, and violation of state privacy laws. If the Board elects for the Company to press forward with its right of action against any of the members of the Board in this action, Target's efforts would directly compromise its defense of the pending consumer class actions. Accordingly, demand on the Board is excused as futile.

DAMAGES TO THE COMPANY

96. As a direct and proximate result of the Individual Defendants' misconduct, Target failed to maintain proper internal controls, caused the Company to release false and misleading statements, caused the Company to pay large sums of money for credit monitoring services for affected customers, caused the Company to be exposed to millions of dollars of potential liability in class action lawsuits, and substantially damaged the Company's sales during the 2013 holiday season, its market capitalization, goodwill, consumer confidence, and brand trust.

97. Furthermore, Target has expended and will continue to expend significant sums of money. Such expenditures include but are not limited to:

a. costs incurred from the Company's internal investigation into the data breach, but not limited to, expense for legal, investigative, and consulting fees;

b. costs of updating customers of the status of the breach;

c. costs incurred from providing credit monitoring for 110 million affected customers;

d. costs incurred from defending and settling the numerous class action lawsuits being brought against the Company for the breach;

e. costs incurred from notifying customers, replacing cards, sorting improper charges from legitimate charges, and reimbursing customers for fraudulent transactions (early estimates put this at roughly $5.10 per card, or $561 million);

f. costs incurred from the Secret Service, DOJ, and U.S. Senate investigations into the data breach, including, but not limited to, liability for any potential fines;

g. costs incurred from notifying customers and rectifying secondary breach caused by imitation credit monitoring emails;

h. loss of revenue and profit resulting from Target's offer of a 10% discount to U.S. shoppers during the last weekend before Christmas in an effort to lure customers back into its stores;

i. costs incurred from instituting chip-based credit cards that will enhance security; and

j. costs incurred from compensation and benefits paid to the defendants who have breached their duties to Target.

98. Moreover, these actions have irreparably damaged Target's corporate image and goodwill such that all Target stores and financial services are associated with failing to protect customer's sensitive information and then keeping that broken promise a secret from customers.

COUNT I

DERIVATIVELY AGAINST ALL DEFENDANTS FOR BREACH OF FIDUCIARY DUTY

99. Plaintiff incorporates by reference and re-alleges each and every allegation contained above, as though fully set forth herein.

100. The Individual Defendants owed and owe Target fiduciary obligations. By reason of their fiduciary relationships, the Individual Defendants owed and owe Target the highest obligation of loyalty, good faith, due care, oversight, fair dealing, and candor.

101. All of the Individual Defendants violated and breached their fiduciary duties of loyalty, good faith, due care, oversight, fair dealing, and candor.

102. Each of the Individual Defendants had actual or constructive knowledge that they had caused Target to maintain improper security controls of customer data and to make false and misleading statements about the data breach once it occurred. These actions could not have been a good faith exercise of prudent business judgment to protect and promote the Company's corporate interests.

103. The Individual Defendants caused or allowed Target to lack requisite internal controls, and, as a result, the Company allowed the worst data breach of customer information in retail history.

104. The Individual Defendants failed to supervise, and to ensure adequate internal controls over, and consciously disregarded responsibilities involving, the Company.

105. The Individual Defendants caused or allowed the scope of the breach to be materially misstated and misrepresented.

106. As a direct and proximate result of the Individual Defendants' failure to perform their fiduciary obligations, Target has sustained significant damages. As a result of the misconduct alleged herein, the Individual Defendants are liable to the Company.

COUNT II

DERIVATIVELY AGAINST ALL DEFENDANTS FOR GROSS MISMANAGEMENT

107. Plaintiff incorporates by reference and re-alleges each and every allegation contained above, as though fully set forth herein.

108. By their actions alleged herein, the Individual Defendants abandoned and abdicated their responsibilities and fiduciary duties with regard to prudently managing the assets and business of Target in a manner consistent with the operations of a publicly held corporation.

109. The Individual Defendants caused or allowed Target to lack requisite internal controls, and as a result, the Company allowed the worst data breach in retail history and then released a series of false and misleading statements about the gravity of the breach.

110. The Individual Defendants caused or allowed the Company's statements to be materially misstated due to the Individual Defendants' failure to properly account for the Company's motives of withholding information from the public in order to protect sales figures.

111. The Individual Defendants failed to supervise, and to exert internal controls over, and consciously disregarded responsibilities involving the Company's public statements, as well as the Company's cyber-security systems.

112. The Individual Defendants caused or allowed the scope of the breach to be materially misstated.

113. The Individual Defendants, including members of the Audit Committee, did not take seriously their primary responsibility for the Company's statistical and financial reporting activities.

114. As a direct and proximate result of the Individual Defendants' gross mismanagement and breaches of duty alleged herein, Target has sustained significant damages that will likely exceed hundreds of millions of dollars.

115. As a result of the misconduct and breaches of duty alleged herein, the Individual Defendants are liable to the Company.

COUNT III

DERIVATIVELY AGAINST ALL DEFENDANTS FOR WASTE OF CORPORATE ASSETS

116. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above, as though fully set forth herein.

117. As alleged herein, the Individual Defendants' wrongful conduct alleged included the failure to implement adequate internal controls to detect and prevent the breach of the Company's customers' personal and financial information. Under the Individual Defendants' supervision, Target's customers became the victims of the worst data breach in retail history.

118. The Individual Defendants caused Target to waste its valuable corporate assets by paying improper compensation and bonuses to certain of its executive officers and directors that breached their fiduciary duty.

119. As a result of the waste of corporate assets, the Individual Defendants are liable to the Company.

COUNT IV

DERIVATIVELY AGAINST ALL DEFENDANTS FOR ABUSE OF CONTROL

120. Plaintiff incorporates by reference and re-alleges each and every allegation contained above, as though fully set forth herein.

121. The Individual Defendants' misconduct alleged herein constituted an abuse of their ability to control and influence Target, for which they are legally responsible. Among the abuses of control was: (i) the Individual Defendants' failure to supervise, and to exert internal controls over, and conscious disregard of responsibilities involving maintenance of proper cyber-

security systems to protect customer personal and financial data and (ii) the Individual Defendants' reckless and/or grossly negligent failure to properly utilize the proper resources to determine whether customer data was safe within the Company's electronic systems.

122. As a direct and proximate result of defendants' abuse of control, Target has sustained significant damages.

123. As a result of the misconduct alleged herein, defendants are liable to the Company.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, demands judgment as follows:

A. Against all of the Individual Defendants and in favor of Target for the amount of damages sustained by the Company as a result of the Individual Defendants' breaches of fiduciary duty, gross mismanagement, waste of corporate assets, and abuse of control;

B. Directing Target to take all necessary actions to reform and improve its corporate governance and internal procedures to comply with applicable laws and to protect the Company and its shareholders from a repeat of the damaging events described herein;

C. Awarding to Target restitution from the Individual Defendants, and each of them, and ordering disgorgement of all profits, benefits, and other compensation obtained by the Individual Defendants;

D. Awarding the Plaintiff the costs and disbursements of this action, including reasonable attorneys' fees, accountants' and experts' fees, costs and expenses; and

E. Granting such other and further equitable relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff demands a trial by jury.

Dated: January 29, 2014

ANDERSON HELGEN DAVIS & NISSEN, P.A.

s/Amanda R. Cefalu
Amanda R. Cefalu, Esq.
333 South Seventh Street, Ste. 310
Minneapolis, MN 55402
Telephone: (612) 435-6349
Facsimile: (612) 435-6379

FARUQI & FARUQI, LLP
Beth A. Keller, Esq.
Todd H. Henderson, Esq.
369 Lexington Avenue, 10th Floor
New York, New York 10017
Telephone: (212) 983-9330
Facsimile: (212) 983-9331

-and-

FARUQI & FARUQI, LLP
Michael J. Hynes, Esq.
Ligaya Hernandez, Esq.
101 Greenwood Avenue, Suite 600
Jenkintown, Pennsylvania 19046
Telephone: (215) 277-5770
Facsimile: (215) 277-5771

Attorneys for Plaintiff

VERIFICATION

I, Maureen Collier, hereby declare as follows:

I am the plaintiff in the within entitled action. I have read the Verified Shareholder Derivative Complaint. Based upon discussions with and reliance upon my counsel, and as to those facts of which I have personal knowledge, the Complaint is true and correct to the best of my knowledge, information, and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Signed and Accepted:

_____

Dated: January __, 2014