

BARBARA BOXER, CALIFORNIA
BILL NELSON, FLORIDA
MARIA CANTWELL, WASHINGTON
MARK PRYOR, ARKANSAS
CLAIRE McCASKILL, MISSOURI
AMY KLOBUCHAR, MINNESOTA
MARK WARNER, VIRGINIA
MARK BEGICH, ALASKA
RICHARD BLUMENTHAL, CONNECTICUT
BRIAN SCHATZ, HAWAII
EDWARD MARKEY, MASSACHUSETTS
CORY A. BOOKER, NEW JERSEY

JOHN THUNE, SOUTH DAKOTA
ROGER F. WICKER, MISSISSIPPI
ROY BLUNT, MISSOURI
MARCO RUBIO, FLORIDA
KELLY AYOTTE, NEW HAMPSHIRE
DEAN HELLER, NEVADA
DAN COATS, INDIANA
TIM SCOTT, SOUTH CAROLINA
TED CRUZ, TEXAS
DEB FISCHER, NEBRASKA
RON JOHNSON, WISCONSIN

United States Senate

COMMITTEE ON COMMERCE, SCIENCE,
AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEB SITE: <http://commerce.senate.gov>

ELLEN DONESKI, STAFF DIRECTOR

DAVID SCHWIETERT, REPUBLICAN STAFF DIRECTOR

January 28, 2014

Mr. Gregg Steinhafel
Chairman, President, and Chief Executive Officer
Target Corporation
1000 Nicollet Mall
Minneapolis, MN

Dear Mr. Steinhafel:

I am writing to inquire why your company has not yet reported the massive data breach Target recently suffered to the Securities and Exchange Commission (SEC). Since 2011, the SEC has recommended that publicly traded companies disclose significant cybersecurity incidents to their investors. Your company does not appear to have followed this guidance, which was intended to give investors complete, timely, accurate information about companies' investment risks.

On October 13, 2011, the SEC's Division of Corporate Finance issued a Disclosure Guidance ("the guidance") discussing publicly traded companies' obligations to disclose cybersecurity risks and incidents. The guidance explained that cyber attacks are a growing source of financial and operational risk to publicly traded companies, and that companies have an obligation to disclose "timely, comprehensive, and accurate information" about risks and events "that a reasonable investor would consider important to an investment decision."¹ The guidance instructed companies to describe their material cybersecurity risks and incidents in a manner sufficiently detailed and specific for investors to appreciate the nature of the risks. An example provided in the guidance appears to precisely describe the data breach your company recently suffered.

For example, if a registrant experienced a material cyber attack in which malware was embedded in its systems and customer data was compromised, it likely would not be sufficient for the registrant to disclose that there is a risk that such an attack may occur. Instead, as part of a broader discussion of malware or other similar attacks that pose a particular risk, the registrant may need to discuss the occurrence of the specific attack and its known and potential costs and other consequences.²

¹ Securities and Exchange Commission, CF Disclosure Guidance, Topic No. 2: Cybersecurity (Oct. 13, 2011) (online at <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>)

² *Id.*

Mr. Gregg Steinhafel
January 28, 2014

Because cyber attacks represent one of the greatest threats to our economic and national security, I encouraged the SEC to issue the guidance in 2011.³ More recently, I have encouraged current SEC Chairman Mary Jo White to issue this guidance at the Commission level.⁴ The President's Council of Advisors on Science and Technology also supports more cybersecurity risk disclosure, recommending in their most recent report that the SEC should require disclosure of cybersecurity risks "that go beyond current materiality tests."⁵ More accurate and complete cybersecurity risk disclosures will give investors a clearer picture of these risks before they purchase stock in a company or exercise their shareholders' rights. Moreover, disclosing these risks to investors gives responsible companies a strong incentive to protect their networks from attacks.

Given the current SEC guidance and the massive scale of the cyber attack your company suffered in late 2013, I am surprised that your company has not provided shareholders with an accurate accounting of the cyber attack and its financial impact on Target's operations. Your company's most recent SEC 10-K filing mentions the following risk:

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 . . . our guests could lose confidence . . . [and] the loss of confidence from a significant data security breach involving team members could hurt our reputation . . . and affect how we operate our business.⁶

A data breach involving the theft of personal information about tens of millions of Target customers is clearly a material cyber attack that has affected how your business operates. I am therefore puzzled why your company has not yet updated its SEC filings to reflect this event. Your failure thus far to provide this information to your investors does not seem consistent with the spirit or the letter of the SEC's financial disclosure rules.

³ Letter from John D. Rockefeller IV to Mary Schapiro, Chairman of the Securities and Exchange Commission (May 11, 2011) (online at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=4ceb6c11-b613-4e21-92c7-a8e1dd5a707e).

⁴ Letter from John D. Rockefeller IV. to Mary Jo White, Chairman of the Securities and Exchange Commission (Apr. 9, 2013) (online at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51).

⁵ President's Council of Advisors on Science and Technology, *Report to the President: Immediate Opportunities for Strengthening the Nation's Cybersecurity* (Nov. 2013) (online at http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf).

⁶ Target Corporation, United States Securities and Exchange Commission Form 10-K (Mar. 20, 2013) (online at <http://www.sec.gov/Archives/edgar/data/27419/000104746913003100/a2213506z10-k.htm>).

Mr. Gregg Steinhafel
January 28, 2014

Please explain to me why Target appears to be ignoring SEC rules that require you to disclose to the SEC and your investors the costs and business consequences of this recent data breach. If you are not ignoring these rules, please let me know when your company expects to make this required disclosure.

I look forward to your response.

Sincerely,

A handwritten signature in black ink, appearing to read "John D. Rockefeller IV". The signature is fluid and cursive, with a prominent initial "J" and a long, sweeping underline.

John D. Rockefeller IV
Chairman