

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

JOHN L. MICA, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN J. DUNCAN, JR., TENNESSEE
PATRICK T. McHENRY, NORTH CAROLINA
JIM JORDAN, OHIO
JASON CHAFFETZ, UTAH
TIM WALBERG, MICHIGAN
JAMES LANKFORD, OKLAHOMA
JUSTIN AMASH, MICHIGAN
PAUL A. GOSAR, ARIZONA
PATRICK MEEHAN, PENNSYLVANIA
SCOTT DESJARLAIS, TENNESSEE
TREY GOWDY, SOUTH CAROLINA
BLAKE FARENTHOLD, TEXAS
DOC HASTINGS, WASHINGTON
CYNTHIA M. LUMMIS, WYOMING
ROB WOODALL, GEORGIA
THOMAS MASSIE, KENTUCKY
DOUG COLLINS, GEORGIA
MARK MEADOWS, NORTH CAROLINA
KERRY L. BENTIVOLIO, MICHIGAN
RON DESANTIS, FLORIDA

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
FACSIMILE (202) 225-3974
MINORITY (202) 225-5051

<http://oversight.house.gov>

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPEIER, CALIFORNIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
MARK POCAN, WISCONSIN
L. TAMMY DUCKWORTH, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY CARDENAS, CALIFORNIA
STEVEN A. HORSFORD, NEVADA
MICHELLE LUJAN GRISHAM, NEW MEXICO

LAWRENCE J. BRADY
STAFF DIRECTOR

January 14, 2014

The Honorable Darrell E. Issa
Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

Since last October, the Committee's top priority has been investigating the security of the Healthcare.gov website and the risks posed by domestic hackers, foreign entities, and others seeking to harm our national interests. This investigation has involved numerous public hearings, tens of thousands of documents obtained from federal agencies and private contractors, and multiple transcribed interviews. Thankfully, to date there have been no successful security attacks against the Healthcare.gov website, although the increasing frequency and sophistication of attacks against all federal information technology systems increases the risks of such a breach.

Unfortunately, while the Committee was conducting its investigation during this time period last fall, up to 110 million Americans were subjected to one of the most massive information technology breaches in history when their credit, debit, and other personal information reportedly was compromised at Target stores and online in November and December.¹

I am writing to request that the Committee hold a bipartisan hearing with senior Target officials and security experts to investigate the cause of this breach, its implications for American consumers, and the steps Target has taken to address this specific breach and implement mitigation measures to ensure that similar attacks are not successful in the future. In addition to serving the interests of millions of American consumers affected by this breach, I believe the Committee could learn from these witnesses about their failures, successes, and best practices in order to better secure our federal information technology systems.

According to security experts, "the kind of information stolen—including names, card numbers, expiration dates and three-digit security codes—could allow criminals to make

¹ *For Target, the Breach Numbers Grow*, New York Times (Jan. 10, 2014) (online at www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?_r=0).

fraudulent purchases almost anywhere in the world.”² Millions of these stolen credit and debit accounts reportedly “have been flooding underground black markets in recent weeks.”³ Based on recent news accounts, it is unclear why Target had inadequate security measures in place,⁴ why the breach was not detected sooner,⁵ and whether the full extent of the breach has been uncovered.⁶

One of the most significant questions is why Target did not notify customers sooner.⁷ Although initial accounts in December reported that approximately 40 million consumers had been affected,⁸ it was reported in January that more than 100 million consumers may have been affected.⁹

You and other House Members have cited the Target breach to justify legislation relating to the Healthcare.gov website. Last Friday, during floor debate on H.R. 3811, The Health Exchange Security and Transparency Act, the bill’s sponsor, Rep. Joseph Pitts, began debate on the bill by stating:

Mr. Speaker, in the days leading up to Christmas, hackers stole millions of credit card numbers from the servers of retail giant, Target. I imagine that at least a few here in this chamber may have had their own credit cards replaced to prevent theft. What if Target had not bothered to tell anyone? What if they had waited until people noticed

² *Target Says 40 Million Credit, Debit Cards May Have Been Compromised in Security Breach*, Washington Post (Dec. 19, 2013) (online at www.washingtonpost.com/business/technology/target-data-breach-affects-40-million-accounts-payment-info-compromised/2013/12/19/5cc71f22-68b1-11e3-ae56-22de072140a2_story.html).

³ *Target Data Breach Spurs Lawsuits, Investigations*, USA Today (Dec. 23, 2013) (online at www.usatoday.com/story/money/business/2013/12/22/target-breach-suits-and-investigations/4167977).

⁴ *Id.*

⁵ *Target Cyber Breach Hits 40 Million Payment Cards at Holiday Peak*, Reuters (Dec. 19, 2013) (online at www.reuters.com/article/2013/12/19/us-target-breach-idUSBRE9BH1GX20131219).

⁶ *Target Says Data Breach is Far Larger Than First Estimated*, Los Angeles Times (Jan. 10, 2014) (online at www.latimes.com/business/la-fi-target-breach-20140111,0,987578.story#axzz2qKAGcErR).

⁷ *Why Did Target Take So Long to Report Data Security Breach?*, CNBC (Dec. 20, 2013) (online at www.nbcnews.com/business/why-did-target-take-so-long-report-data-security-breach-2D11783300).

⁸ *Target Says 40 Million Credit, Debit Cards May Have Been Compromised in Security Breach*, Washington Post (Dec. 19, 2013).

⁹ *For Target, the Breach Numbers Grow*, New York Times (Jan. 10, 2014) (online at www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html).

fraudulent charges popping up on their statements? The damage would certainly be worse.

Later in the debate, you invoked the Target breach, stating: "no private sector company, including Target, would go live with a system that has known failures and unknown failures because of a failure to do end-to-end."

During a television interview yesterday, Target's Chief Executive Officer, Gregg Steinhafel, explained his company's approach to handling this crisis:

As time goes on, we are going to get down to the bottom of this. We are not going to rest until we understand what happened and how that happened. Clearly, we are accountable, and we are responsible. But we are going to come out at the end of this a better company. And we're going to make significant changes. I mean, that's what you do when you go through a period like this. You have to learn from it, and you have to apply those learnings. And we're committed to do that.¹⁰

I believe this is a positive overall approach, but it will take oversight to ensure that the company follows through on its responsibilities. As Majority Whip Kevin McCarthy stated in the context of the Healthcare.gov website: "Nothing can turn a life upside down more quickly than identity theft. It is our duty to do everything we can to inform Americans."¹¹

For these reasons, I request that the Committee engage with Target, in a collaborative and bipartisan way, not only to help protect the millions of consumers affected by this massive breach, but to learn lessons that can help us improve federal information technology systems and procedures.

Thank you for your consideration of this request.

Sincerely,



Elijah E. Cummings
Ranking Member

¹⁰ *Squawk Box*, CNBC (Jan. 13, 2014) (online at <http://video.cnbc.com/gallery/?video=3000235005>).

¹¹ *House Passes Obamacare Security Measure*, Politico (Jan. 10, 2014) (online at www.politico.com/story/2014/01/house-passes-obamacare-security-measure-102018.html).