

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

July 20, 2015

The Honorable Gene Dodaro
Comptroller General
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Comptroller General Dodaro:

In the last several years, we have seen numerous reports of massive data breaches involving Americans' personal information. Data breaches can result in personal information being acquired by cybercriminals to perpetrate identity theft, which can lead to financial consequences for victims – both individuals and the entities that are breached – and can take months or sometimes years to resolve. Unfortunately, neither the private sector nor the federal government have been immune to these breaches.

For example, in 2013, up to 70 million Target customers may have had their credit card and other information stolen.¹ In August 2014, JPMorgan Chase disclosed that a cyberattack on its systems compromised the information of 76 million households and seven million small businesses.² A cyberattack of thousands of Home Depot stores in 2014 compromised 56 million credit cards.³ And health insurer Anthem suffered a December 2014 breach of up to 80 million customers' names, Social Security numbers, and other data.⁴

Similarly, several high profile breaches at federal agencies have potentially comprised personal information. For example, in May 2012, hackers accessed data on 123,000 participants from the Federal Thrift Savings Plan.⁵ In July 2013, the personal information of 140,000 individuals, which included birthdates, bank accounts, and Social Security numbers, was

¹ *Data breach FAQ*, Target (accessed June 29, 2015).

² Matthew Goldstein, Nicole Perlroth and Michael Corkery, *Neglected Server Provided Entry for JPMorgan Hackers*, New York Times (Dec. 22, 2014).

³ Robin Sidel, *Home Depot's 56 Million Card Breach Bigger Than Target's*, Wall Street Journal (Sept. 18, 2014).

⁴ Elizabeth Weise, *Massive breach at health care company Anthem Inc.*, USA Today (Feb. 5, 2015).

⁵ Senate Committee on Homeland Security and Governmental Affairs, Testimony of Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office, *Hearing on Data Breach on the Rise: Protecting Personal Information from Harm*, 113th Cong. (Apr. 2, 2014).

removed from a Department of Energy system.⁶ The U.S. Postal Service disclosed in November 2014 that a hack of employee data potentially affected over 750,000 employees.⁷ Finally, the recent series of breaches at the Office of Personnel Management resulted in the potential loss of data for tens of millions of current and former federal employees.⁸

In all of these cases, part of the response by the breached entities has included an offer of free credit monitoring services for varying lengths of time. Questions have been raised, however, about the usefulness and adequacy of credit monitoring services in protecting victims' credit following a breach. For example, according to experts, some credit monitoring services only monitor one of the three major credit bureaus, while criminals know to apply for credit at all three bureaus.⁹ Experts have also questioned whether one to two years of credit monitoring offers sufficient protection since cyber criminals can use stolen personal information many years after monitoring services have expired.¹⁰

In addition to credit monitoring, these post-breach packages can also include other services, such as identity theft insurance, Internet surveillance, and identity theft restoration assistance. The usefulness of these services has also been questioned.¹¹ Moreover, in 2010, the practices of a fraud detection service company led to an investigation by the Federal Trade Commission (FTC) and state attorneys general, resulting in a \$12 million settlement for charges that the company used false claims to promote its identity theft protection services.¹²

We therefore request that the Government Accountability Office undertake a review of credit monitoring and other post-breach identity theft services and provide recommendations to enhance consumer protection. The committee requests that GAO focus on the following questions:

1. At present, how do the federal government and private sector evaluate the success and effectiveness of post-breach consumer protection services?
 - a. Which government agencies conduct such evaluations? Which companies that offer these services evaluate their own services? Which independent companies or organizations evaluate these services?
 - b. What information is reviewed as part of these evaluations?

⁶ *Id.*

⁷ Evan Perez, *Massive Postal Service breach hits employees and customers*, CNN (Nov. 10, 2014).

⁸ Evan Perez and Shimon Prokupez, *U.S. data hack may be 4 times larger than the government originally said*, CNN (June 23, 2015).

⁹ See e.g., Brian Krebs, *Are Credit Monitoring Services Worth It?* Krebs on Security (Mar. 19, 2014); Margot Roosevelt, *Does Anthem's identity protection plan leave victims vulnerable?*, Orange County Register (Mar. 19, 2015); Andrea Peterson, *Data exposed in breaches can follow people forever. The protections offered in their wake don't*, Washington Post (June 15, 2015); Eric Katz, *Why Credit Monitoring Fails to Address the Real Threat Facing Hacked Feds*, Government Executive (June 11, 2015); Kathleen Burke, *'Free credit monitoring' after data breaches is more sucker than succor*, Market Watch (June 10, 2015).

¹⁰ *Id.*

¹¹ *Id.*; Consumer Reports, *Don't get taken guarding your ID* (Jan. 2013).

¹² Federal Trade Commission, *LifeLock Will Pay \$12 Million to Settle Charges by the FTC and 35 States That Identity Theft Prevention and Data Security Claims Were False* (Mar. 9, 2010) (press release).

2. What post-breach services are available to consumers and to breached entities? Describe with specificity each service provided. Which services provide the most benefits for consumers?
 - a. How are these types of post-breach services typically offered, e.g., as bundled packages, as separate services? How are these services priced for individual consumers? How are they priced for private breached entities? How are they priced for breached entities in the federal government?
 - b. How do private and/or federal breached entities determine which of these services to purchase and offer to their customers whose personal information was compromised in a security breach?
3. How do consumer protection services evaluate and keep pace with evolving threats associated with identity theft and consumer fraud?
4. How are consumers informed of the benefits and limitations of free credit monitoring and other post-breach identity-theft protections?
5. How does the federal government ensure taxpayer dollars are being spent effectively for post-breach services?
6. To what extent could the use of these services and the information they compile create further vulnerabilities for the disclosure of personal information? Are there any standards or regulations governing third-party data sharing by these entities?

Thank you for your assistance with this matter. If you have any questions, please contact Ryan Gottschall at (202) 225-3641 or Melissa Froelich at (202) 225-2927.

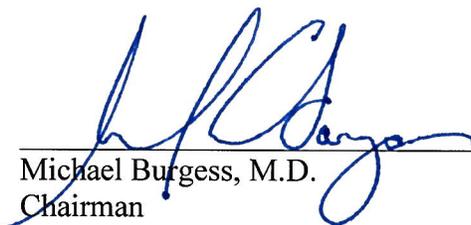
Sincerely,



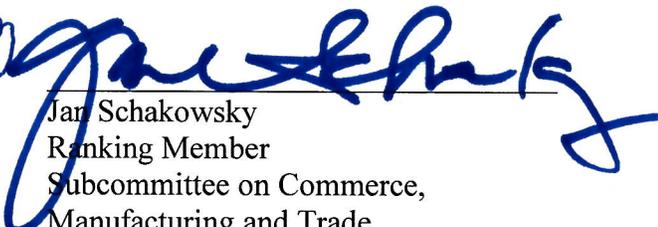
Fred Upton
Chairman



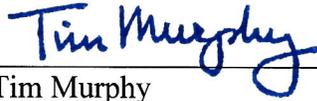
Frank Pallone, Jr.
Ranking Member



Michael Burgess, M.D.
Chairman
Subcommittee on Commerce,
Manufacturing and Trade



Jan Schakowsky
Ranking Member
Subcommittee on Commerce,
Manufacturing and Trade



Tim Murphy
Chairman
Subcommittee on Oversight
and Investigations



Diana DeGette
Ranking Member
Subcommittee on Oversight
and Investigations