FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

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 9, 2015

The Honorable Edith Ramirez
Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chairwoman Ramirez:

In the last several months, we have seen numerous reports about data breaches affecting American families. More than 70 million people report their personal information was compromised in 2014.[1] By one estimate, between 60 and 80 percent of Social Security numbers have been stolen by hackers.[2] While we continue to be concerned about preventing breaches and notifying consumers when their data is at risk, we are also concerned with the efficacy of measures to protect consumers whose personal information has been compromised by a breach.

In many of the high-profile breaches over the past several years, breached entities have offered free credit monitoring services for approximately 12 months to affected customers.[3] However, a number of cybersecurity experts and consumer advocates have raised questions about whether 12 months of credit monitoring is the appropriate response.[4]

It is also unclear if those affected by a breach are sufficiently aware of the options available to them post-breach and whether those options are effective in preventing further financial consequences.

In addition, there can be a mismatch between the types of information lost and the services offered post-breach. Breached entities may offer credit monitoring services, which can

---

[1] Donna Tapellini, *70 Million Americans Report Stolen Data*, Consumer Reports (May 7, 2015).
[2] Aarti Shahani, *Theft of Social Security Numbers is Broader Than You Might Think*, NPR (June 15, 2015).
[3] Kathleen Burke, *'Free credit monitoring' after data breaches is more sucker than succor*, Market Watch (June 10, 2015).
[4] Brian Krebs, *Are Credit Monitoring Services Worth It?*, Krebs on Security (Mar. 19, 2014); 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); House Committee On Energy and Commerce, *Hearing on Understanding the Cyber Threat and Implications For the 21st Century Economy*, 114th Cong. (Mar. 3, 2015).

be helpful for a stolen Social Security number, but not helpful for fraudulent credit card charges. Moreover, credit monitoring services detect indicators of identity theft once they have occurred. Those services do not prevent identity theft.[5] They are also limited because they typically only monitor one of the three major credit bureaus, and criminals know to apply for credit at all three bureaus.[6]

As an alternative – or addition – to credit monitoring, consumers can freeze their credit as a post-breach protection. A credit freeze, or security freeze, offers consumers the option to lock access to their credit from anyone attempting to open new lines of credit in their names.[7] While credit monitoring does not detect fraudulent activity until after it occurs, a security freeze may prevent fraudulent activity by making it more difficult to use stolen information to open new lines of credit.[8]

Currently, consumers must separately request a credit freeze at each of the three credit bureaus.[9] They are then responsible for maintaining separate PIN numbers for each bureau to unlock their credit.[10] Modest fees are usually associated with setting up, lifting, and removing a freeze at each of the bureaus. In many states, a free security freeze requires an individual to produce a police report or affidavit to prove he or she was the victim of identity theft.[11] While some states prohibit fees for certain transactions, there is wide variation among state laws. Some states also automatically remove the freeze after a certain number of years.[12]

It may be possible to streamline the process to reduce fraud following a breach. Therefore, we are writing to learn more about consumer-friendly post-breach protections, including whether the process of activating and inactivating a credit freeze can be made more efficient and less costly.

As we examine the security freeze process and other post-breach tools available to consumers, we are writing to ask you to respond to the following questions:

1) Do you have evidence that consumers are currently aware of the option to freeze their credit to prevent their information from being used by cyber criminals to establish new lines of credit? Has your agency received any feedback from consumers about the current security freeze laws? If so, what is that feedback?

---

[5] Andrea Peterson, *Data exposed in breaches can follow people forever. The protections offered in their wake don't*, Washington Post (Jun 15, 2015).
[6] *See* note 3.
[7] *Consumers Union's Guide to Security Freeze Protection*, Consumers Union (Feb. 5, 2014).
[8] Anthony Giorgianni, *Should You Freeze Your Credit File?*, Consumer Reports (Feb. 22, 2014).
[9] Ron Lieber, *Identity Theft Poses Extra Troubles for Children*, New York Times (Apr. 17, 2015).
[10] *See* note 8.
[11] *See* note 8; Free credit freezes are also available to seniors over the age of 65 in many states. *Consumers Union's Guide to Security Freeze Protection*, Consumers Union (Feb. 5, 2014).
[12] *See* note 8.

2) What, if any, are the regulatory or legislative mechanisms available to reduce the cost of security freezes for consumers? What initiatives are available to relieve the consumer from the cost of setting up and lifting a freeze?

3) Has the Federal Trade Commission explored federal standards for security freezes? What are the existing obstacles to expanding the use of security freezes? How can those obstacles be overcome?

4) How can the security freeze process be streamlined, including for parents seeking to freeze the credit of their minor children? How can we make it easier for consumers to place a security freeze at each of the credit bureaus? Could a model like AnnualCreditReport.com be used for this purpose? Are there costs or possible unintended consequences associated with increasing consumer access to security freezes?

5) How can federal regulatory or legislative efforts regarding security freezes account for consumers who do not have a credit report? How can consumers who are "credit invisible" initiate a security freeze? What other options might these credit invisible consumers have to protect themselves following a breach?

6) Beyond the credit freeze, are there other protections that are available or can be made available to consumers following a breach of their personal information? For example, is credit monitoring considered a best practice in this area, and what is an appropriate length of time for breached entities to provide credit monitoring following a breach?

We ask that you provide a briefing to committee staff on these issues and other methods to improve post-breach protections no later than July 20, 2015. Please contact Elizabeth Letter or Ryan Gottschall at (202) 225-3641, or Paul Nagle or Melissa Froelich at (202) 225-2927 if you have any questions.

Sincerely,

Fred Upton
Chairman

Frank Pallone, Jr.
Ranking Member

Michael Burgess, M.D.

Jan Schakowsky

Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

Ranking Member
Subcommittee on Commerce,
Manufacturing, and Trade

Tim Murphy

Tim Murphy
Chairman
Subcommittee on Oversight
and Investigations

Diana DeGette

Diana DeGette
Ranking Member
Subcommittee on Oversight
and Investigations