GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH 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

August 30, 2017

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

Dear Mr. Dodaro:

As you know, many entities in the private and government sectors have experienced data breaches involving the loss or theft of sensitive personal information, such as Social Security numbers, fingerprints and credit card information. Recent trends suggest information-rich institutions remain major targets, and unscrupulous actors will continue to exploit vulnerabilities in information security systems.

A popular response to these breaches has been to provide affected consumers with credit monitoring services. However, questions remain about whether purchasing and providing credit monitoring for customers is the optimal way to respond to data breaches. In particular, we are concerned that the popular response may reflect factors unrelated to the actual protection of breach victims and reliance on these products after the breach may result in consumers being lulled into a false sense of security.

For example, GAO recently issued a report, entitled *Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud (GAO-17-254)*, in response to a request from the House Energy and Commerce Committee. This report found that some breached private companies offer consumers identity theft services for reasons independent of the effectiveness of the services, such as to avoid liability or to offer consumers "peace of mind," even in a case where the services did not necessarily address the risks associated with a particular breach. The GAO report also found the Office of Management and Budget's (OMB) guidance to agencies on preparing for and responding to breaches of personally identifiable information does not address a service's effectiveness, and may not fully reflect the most useful and cost-effective options agencies should consider in response to a breach.

Moreover, GAO's recent report on synthetic ID fraud (GAO-17-780SP) sheds light on how fraudsters create and build synthetic identities through the credit ecosystem that can leave children, the elderly and the unbanked particularly vulnerable. These findings raise questions as

to whether private-sector and government entities have converged on suboptimal solutions for providing protection for costumers and whether better solutions ought to be pursued.

Therefore, we request GAO to conduct work that will help us determine the most effective way to offer more robust protections for customers and better understand barriers to more effective solutions. Specifically, we are requesting that GAO provide information on the following questions:

1. Which of the existing solutions provide reasonable protections for breach victims using criteria GAO deems appropriate? For example, are particular solutions more effective than others or more cost-effective?

    a. What are the most commonly offered services, including credit monitoring, and how specifically do those services work? For example, are all credit bureaus monitored and for how long?
    b. To what extent are fraud alerts and credit freezes offered? What protections do they provide to consumers in the wake of a breach? Why are credit freezes and fraud alerts not a default option for breached entities?
    c. To what extent does the most effective solution vary by breach type, victim characteristics, demographics or other key factors? What is the range of solutions that should be offered for each type of breach?
    d. To what extent are the services offered determined by price? To what extent are they determined by their level of protection?

2. What additional options not currently being used or considered are potentially feasible?
    a. What are the benefits of these options?
    b. What unintended consequences or drawback to these alternatives need to be considered?

3. While credit cards continue to be stolen, other information such as the detailed background checks of federal employees are becoming more common targets for theft. What are the recent trends in breaches or information theft?
    a. How should we review post-breach services in light of these new threats?
    b. Are breached entities considering the threats beyond identity theft?

4. To the extent that GAO identifies effective post-breach solutions and obstacles that impede their use, what can the federal government and the private sector do to make these solutions easier to leverage?

Our Committee staff will work with you to prioritize multiple reports if deemed appropriate. Thank you for your timely attention to this request. If you have any questions, please contact the Democratic Committee staff at (202) 225-3641.

Sincerely,

Frank Pallone, Jr.
Ranking Member

Diana DeGette
Ranking Member
Subcommittee on Oversight
and Investigations

Jan Schakowsky
Ranking Member
Subcommittee on Digital Commerce
and Consumer Protection