4/7/17

By Susan Grant, Consumer Federation of America Director of Consumer Protection and Privacy

After the federal Office of Personnel Management (OPM) experienced two massive data breaches in 2015, it spent about $240 million to provide identity theft services to those affected. Was that money well-spent? To answer that question, Congress asked Government Accountability Office (GAO) to look into identity theft services and their usefulness. The GAO's report concludes that there are both benefits and limitations of these services that should be taken into account when determining how to respond to data breaches. These findings are in line with research that we at Consumer Federation of America (CFA) have done. Last year, CFA issued a checklist, *My company's had a data breach, now what?*, which explains when it might be appropriate to provide identity theft services after a breach and what features to look for to ensure that the victims will get the information and assistance that best fits their needs.

While credit monitoring, which is a common feature in identity theft services, can help to detect new-account fraud, the GAO noted that alternatives such as low-cost credit freezes can actually prevent new account fraud by blocking access to their credit reports. It's unclear how effective other types of monitoring are, such as checking public records or illicit websites where consumers' personal information is trafficked, according to the GAO.

Another common feature of identity theft services is identity restoration. The GAO found that these features vary, from providing consumers with self-help information to offering hands-on assistance to resolve the problems that the identity theft may cause. Identity theft insurance, which is also standard in most identity theft services, typically covers expenses that victims may incur to remedy the situation, within certain limits, but generally don't reimburse them for money stolen from their accounts. The GAO also confirmed what we have long suspected – there aren't many insurance claims and payouts usually just a few hundred dollars, rarely exceeding a few thousand.

In fact, one of the concerns that the GAO cited was that in the wake of the OPM breaches, Congress dictated that it provide victims with $5 million in identity theft insurance. This level of coverage is likely unnecessary, said the GAO, and could not only increase federal costs but mislead consumers about the benefit of such insurance and escalate coverage amounts in the marketplace. Congress should allow agencies to have the flexibility to determine the appropriate amount of insurance coverage, the GAO recommended.

The GAO also recommended that the Office of Management and Budget (OPM), which provides guidance to federal agencies on responding to data beaches, should:

- Analyze the effectiveness of identity theft services relative to lower-cost alternatives such as credit freezes;

- Find ways to avoid providing duplicate identity theft services to breach victims (in the two OPM breaches, 3.6 million people received duplicate services);

- Establish criteria in its breach-response policy for determining when agencies should offer identity theft services.

Businesses and nonprofit organizations might also want to take these recommendations onboard. It makes no sense to provide breach victims with identity theft services without carefully considering, in light of the types of data that have been compromised, what will be most helpful to them.