OPM Data Breach Letter Reveals Extent of Information Stolen on Government Employees and Contractors

October 21, 2015 â€“ The Office of Personnel Management has posted copies of two letters that are being sent out to current and former government employees, contractors and their family members to its website. Prior to the posting, it was well known that the data breach was extensive. But the letters indicate that the hackers behind the breach â€“ believed to the Chinese government â€“ wound up stealing enough information to build detailed portfolios on more than 21 million people; many of whom have government security clearances.

One version of the letter is being sent to 16 million people who had their social security numbers stolen in the breach. It reads, in part, "If you applied for a position or submitted a background investigation form, the information in our records may include your name, Social Security number, address, date and place of birth, residency, educational, and employment history, personal foreign travel history, information about immediate family as well as business and personal acquaintances, and other information used to conduct and adjudicate your background investigation. If your information was listed on a background investigation form by a spouse, or co-habitant, the information in our records may include your name, Social Security number, address, date and place of birth, and in some cases, your citizenship information."

The second version of the letter, being sent to more than 5 million people, is directed at those who went through the security clearance process and who had their digitized fingerprints stolen. In addition to the statement shown above, it includes the following statement: Our records also indicate your fingerprints were likely compromised during the cyber intrusion."

You might think that after a data breach of this extent, the federal government would be pulling out all of the stops to help protect those victimized in the breach. But the weak response to the breach makes it quite apparent that OPM and the rest of the federal government really donâ€™t know how to respond.

Three years of credit monitoring is apparently the extent of the assistance being provided to victims. If you read our postings regularly, you probably know that ACCESS position on credit monitoring is that it is useless. It only notifies you of a breach after it has occurred and does nothing to help you restore your credit. But our position on credit monitoring is actually based on the idea that if your data is stolen in a data breach, it will be used to commit fraud or steal your identity for other purposes. As previously mentioned, the government believes that the government of China is behind this breach. If that is the case, China isnâ€™t likely to use the stolen data to make a bunch of fraudulent purchases at Macyâ€™s or Best Buy.

A much more likely scenario is that China will use the stolen information to find out which of the 21 million people with stolen data have sensitive jobs within the government. From there, they are likely to try and narrow the field down further to those with both sensitive jobs and who are financially stressed.

So if you are China, and you want have identified several thousand people who are in sensitive positions â€“ some with security clearances â€“ how do you find out if those people are having financial difficulty? Well, the logical place to look would be their credit file.

Knowing this, there are three logical things for the federal government to be doing right now. First, they should be advising victims of the breach to freeze their credit files. Those with security clearances should actually be forced to freeze their credit files in order to maintain their clearance.

This wouldnâ€™t prevent China from getting its hands on the information it is seeking but it would prevent them from using credit inquiries that look legitimate. This is the easiest way for them to get their hands on this information right now and from what we are seeing, the government isnâ€™t doing anything to prevent it.

The second logical step is for the federal government to begin working closely with the credit repositories â€“ Experian, Equifax and TransUnion â€“ on cybersecurity. Specifically, the federal government needs to assist these companies to insure that their systems are secure and be looking for unusual patterns of credit inquiries on government employees.

Finally, the third logical step is for the federal government to be looking at the stolen data the same way that China is. In other words, trying to determine which employees in sensitive positions are vulnerable to manipulation due to their financial circumstances. This should be an ongoing effort. Once those employees are identified, the government would have several options. Those include working with the employees to make them more financially secure, transferring them to other positions and in some cases could include termination.

Perhaps the government is doing some of these things but, based on the posted letters by OPM, it certainly doesnâ€™t look like they are. And if the federal governmentâ€™s abysmal record on cybersecurity to date is any indication, we can almost guarantee you that they arenâ€™t doing much of anything.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS