Effects of Equifax breach will stretch into future

By Hiawatha Bray
GLOBE STAFF

If you're an adult American, there's a very good chance your identity just got stolen. And if you're not worried about it, now would be a good time to start.

The credit reporting company Equifax Inc. said Thursday that a massive breach of the company's computers might have exposed the personal information of 143 million Americans — more than half of the adult population.

"Everyone should assume that their data may have been lost in this breach," said Michael Kaiser, executive director of the National Cyber Security Alliance in Washington. "And everyone should review and make sure they are implementing the most basic cybersecurity practices."

Almost every week brings new reports about major breaches, and they've become so common it's easy to become jaded and indifferent. Last year Yahoo disclosed a breach of 1 billion accounts. The Equifax breach seems trivial by comparison.

But it's not. The Yahoo theft contained little personal information. But the Equifax raid swept up highly sensitive information, the crown jewels of personal identity data: names, Social Security numbers, birthdates, addresses, and, in some instances, driver's license numbers. It may be the worst such theft ever.

Thieves can use that data to impersonate people, obtain credit cards and bank loans in their names, and even file fake claims for tax refunds.

While credit cards can be canceled, names and Social Security numbers cannot. The stolen data can literally last a lifetime.

Equifax said the theft included credit card information for about 209,000 Americans. But Kaiser points out credit card theft is a manageable threat because "credit cards, by their nature, have fairly strong fraud protection."

These include automatic detection of fraudulent purchases and shielding consumers from financial losses if phony charges are reported quickly. Consumers should keep close tabs on their credit and debit card bills, and quickly report any questionable transactions.

The threat of identity theft is more severe. Equifax is offering a monitoring service to inform consumers of any checks of their credit data. Say a criminal tries to obtain a credit card using a stolen name and Social Security number. The card issuer would run a credit check, and the Equifax service would notify the victim that a particular bank was examining his financial records. The victim could immediately contact the bank and warn it not to issue a card under his name.

Consumers are entitled by law to a free copy of their credit reports once a year that can be obtained at annualcreditreport.com; some other services also offer free reports.

Equifax is also offering a total credit freeze that bans any institution from reviewing a user's data without explicit permission.

But the Equifax offer has its limits. When a Globe reporter signed up for it, an on-screen message said coverage wouldn't be available until Sept. 14. And the company won't send an e-mail reminder, but rather users will have to remember to log in and activate the service. Also late Friday Equifax bowed to criticism and clarified that users of its free service would not be signing away their rights to take legal action against the company.

Also, Equifax can only offer a credit freeze on its own database. Criminals could still target businesses that use the other two major credit reporting companies, TransUnion Co. and Experian PLC. Consumers will have to sign up for a credit freeze separately at each, at fees ranging from $5 to $10.

And the Equifax protection is free for just one year, and then costs about $20 a month for a similar level of protection.

Michael Figueroa, executive director of the Advanced Cyber Security Center in Bedford, said temporary monitoring is not effective, because criminals can use the stolen data indefinitely.

"That personal information does not get dated. It uniquely identifies us for our entire lifetime," Figueroa said.

Since banks don't charge extra to monitor and warn customers of irregularities, Figueroa said the three credit reporting companies should provide the same free service for the consumer's entire life.

Kevin Mitnick, chief hacking officer at Florida data security firm KnowB4, said consumers should regularly check with the Internal Revenue Service in case identity thieves use their Social Security numbers to file for phony tax refunds. Consumers can sign up for free downloads of their tax data, to make sure no one else has filed in their names.

Hiawatha Bray can be reached at hiawatha.bray@globe.com. Follow him on Twitter @GlobeTechLab.

9/9/17 Boston Globe

https://www.usatoday.com/story/money/2017/09/11/how-defend-yourseafter-equifax-data-breach-credit-report-freeze-strong-defense-against-identity-thef/654065001/

or

https://www.washingtonpost.com/news/the-switch/wp/2017/09/09/after-the-equifax-breach-heres-how-to-freeze-your-credit-to-protect-your-identity/?utm_term=.3daa8988da1e

or

https://www.usatoday.com/story/money/2017/09/09/equifax-data-breach-could-create-life-long-identity-theft-threat/646765001/

or

https://www.fool.com/credit-cards/2017/09/10/the-equifax-data-breach-is-massive-heres-how-to-pr.aspx

and the excellent article you found as background.