September 2017

WHAT TO DO IF YOU'RE AFFECTED BY THE EQUIFAX DATA BREACH

Earlier this month, Equifax, one of the nation's three largest credit reporting companies, announced a data breach that could affect over 143 million U.S. consumers. First Oklahoma Federal Credit Union reports our credit experiences with you, our valued members, and in turn we occasionally receive information about you when you apply for credit.

While there is no evidence of unauthorized activity in the Equifax credit reporting databases, the company said that there was potential unauthorized access to information it had stored from mid-May through July 2017. The information included names, Social Security numbers, birth dates, addresses and, in some cases, driver's license numbers.

The hackers also got access to credit card numbers for roughly 209,000 consumers, plus certain dispute documents with personal identifying information for approximately 182,000 consumers, Equifax said.

In the wake of this breach, experts counsel several immediate actions:

BE EXTRA CAREFUL ABOUT EMAILS AND LINKS

Users should avoid clicking on links or downloading attachments from suspicious emails that claim to be updates from Equifax or connected to the breach.

Equifax will send paper mail to consumers whose credit card numbers or dispute documents with personally identifying information were impacted. It has also created a dedicated website for consumers to see if they were affected at www.equifaxsecurity2017.com. They can also call the Equifax call center at 866-447-7559.

Hackers often use news of big breaches to conduct "phishing" campaigns, sending official-looking emails that make it seem as if the affected company or other legitimate services are asking them to supply information or click through to a link to repair any damage.

When in doubt, call or email the company that appears to be sending the message separately, don't go through the email you've been sent.

CHANGE PASSWORDS

Especially if you typically use similar passwords and security questions on multiple accounts, do this. Once hackers have access to ID and password information for one system, they routinely try the same combination against multiple other platforms to see which ones work, an easily automated process. If you need assistance re-setting your passwords with any First Oklahoma Federal Credit Union service, please contact us at (918) 582-1965 or (800) 843-9661.

ENABLE TWO-FACTOR AUTHENTICATION

For the vast majority of victims who didn't have credit information compromised, the biggest risk here is that a criminal uses this information to answer your "security questions" and reset your password.

That usually sends a password reset to your email account, so making sure that email account is secure should be your primary concern, said Nathaniel Gleicher, head of cybersecurity strategy for Illumio, and former director of cybersecurity policy for the White House under President Obama.

Two-factor authentication keeps them from doing that by sending a text message or call to the user's phone with a code as a second verification step. The code which must be typed in before the account can be opened.

CHECK YOUR CREDIT CARD AND OTHER ACCOUNTS

Review your online accounts for suspicious activity. That includes banks, credit card companies and hotel and airline loyalty programs. Hackers frequently slice and dice information from large data breaches, selling groups of user information for specific companies on the dark web. Even the smallest accounts can be bundled together into a large group to be sold.

If you have any questions, please contact us here at your credit union.