EQUIFAX DATA SECURITY BREACH: WHAT YOU NEED TO KNOW

Equifax, one of the three major credit reporting agencies, reported that hackers had infiltrated its systems and gained access to sensitive information of 143 million consumers. The NYS Department of Financial Services is reviewing the incident and recommends that those who may be breach victims take steps to protect themselves.

Background

According to Equifax, it discovered the unauthorized access on July 29, 2017. Information accessed by the hackers includes consumers' names, birthdates, Social Security numbers, driver's license numbers, credit card numbers, and "dispute documents" containing personal information. Much is still unknown about the breach and the situation is unfolding daily; Equifax is posting updates on its website.

Equifax has established a website, www.equifaxsecurity2017.com, and a call center, 866-447-7559. Equifax has stated that it is sending direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were breached.

Watch Out for Pretexting Calls, "Phishing" Scams, and Attempts to Profit From the Breach

Impacted consumers should not provide information to anyone who calls them claiming to be from Equifax, or in response to an email (or a link within), as these could be scam emails targeting Equifax breach victims. Such email "phishing" scams, designed to capture personal information like user names, passwords and credit card information and containing links designed to get recipients to click on them, may appear to come from Equifax. Do not click on any links (including links to free credit monitoring) sent to you in an email, or via social media, as any personal information you send through such links will be transmitted to scammers taking advantage of the incident.

Further, consumers should be wary of individuals or entities seeking to profit from the Equifax breach by marketing products tailored to remedy any damage caused, or that may be caused, by the breach.

Consider Taking Actions to Protect Yourself

While many security breaches do not result in identity theft, consumers who may have been affected should consider taking measures to protect themselves.

Security Freeze

A security freeze (also called credit freeze) generally makes it more difficult or impossible for someone to open an account or borrow money in your name using breached information. It prevents creditors from accessing your credit files to review your history, and, as a result, prevents any new credit from being opened in your name, unless you authorize the agencies to allow access by providing the special PIN each agency provides when you sign up. A security freeze will stop all creditors, including legitimate ones, from reviewing your files, unless you allow access by temporarily lifting the freeze. Lifting the freeze takes time, which may present some inconvenience. Consumers who are victims of identity theft, or think they may be victims, should consider placing a freeze.

The procedures for obtaining a freeze are slightly different for each of the three credit reporting agencies, and for a freeze to work you must place one with each of the three agencies. Consumers should call each agency (Experian, 888-397-3742; TransUnion, 888-909-8872; Equifax, 800-349-9960) to place the freeze. Visit their websites (www.transunion.com, www.experian.com, www.equifax.com) to learn details. Credit reporting agencies may require consumers placing a freeze to pay a small fee depending on the agency. If you are an identity theft victim and provide a valid copy of an identity theft report filed with a

law enforcement agency, the fee for placing a freeze will not be required. Consumers should not pay a fee unless it is required.

For more information about a security freeze, visit the Federal Trade Commission's Consumer Information Credit Freeze FAQs.

Fraud Alert

A fraud alert notifies creditors to contact you before they open new accounts or change existing accounts. Unlike a security freeze, a fraud alert does not lock down your credit; while creditors get an alert message, there is no guarantee they will not issue credit. A fraud alert generally lasts for 90 days, although it can be extended.

To place a fraud alert on credit reports, customers should contact one of the three major credit reporting agencies (contact information available by visiting their websites). The agency you place the alert with is required to tell the other two agencies, but to be sure, you might consider placing a fraud alert with all three.

Monitor Your Credit Report, Statements and Disclosures

Checking your credit reports on a regular basis is a good way to spot identity theft soon after it happens. If an identity thief is opening new accounts in your name, those accounts are likely to show up on your report. You may obtain a free credit report from each of the three major credit reporting agencies once a year. Visit www.annualcreditreport.com or call 877-322-8228 to obtain these free reports. Order a report from a different agency every four months, and check it carefully for accounts you did not open and other questionable activity.

You should also closely monitor your credit card, monthly bills, and bank statements on a regular basis. If you see any signs of fraud, report them immediately to the affected organization, both by phone and certified mail. You may ask your bank or credit card company to put a security block on your account or preemptively request a new credit or debit card. You may also want to consider closing affected bank accounts and opening new ones.

Be Wary of Tax Identity Theft

You should also consider filing your taxes as soon as you can. Whenever scammers obtain Social Security numbers, there is the possibility they may use them to commit tax identity theft to get your tax refund. Respond promptly to IRS correspondence.

Commercial Credit Monitoring

Commercial credit monitoring, which generally requires fees or subscriptions, typically monitors your credit report on a regular basis, depending on the product. Its goal is to pick up signs of identity theft and alert you, enabling you to stop identity theft early, but it is not always foolproof. Credit monitoring may lull a consumer into thinking that he/she is protected from identity theft. Further, while they may alert you that your information is being misused, they do not prevent identity theft from occurring and if you believe you are a victim of identity theft, you must take action; the service will generally not act for you. Different services monitor different activities (for example, credit limit increases, new accounts open in your name, changes to public records), depending on the product.

More Information

DFS's informational brochure What You Need to Know About Identity Theft provides general consumer education on identity theft.