EQUIFAX DATA BREACH

What you need to know about protecting your identity

On September 7, 2017, Equifax, one of the largest consumer credit agencies, announced that a data breach took place mid-May through July of this year, potentially affecting 143 million U.S. consumers.[1] The data breach included Social Security numbers, names, addresses, driver's license numbers, dates of birth, and in some cases, credit card numbers.

Equifax published a web page for consumers to visit and determine if their information was included in the breach https://www.equifaxsecurity2017.com. They have also extended identity protection to those involved. However, consumers should also be aware that although Equifax is agreeing to monitor your credit, they are not offering any services to remedy or restore your identity or credit.

Here are specific steps to consider if you're impacted by the Equifax breach, many of which are good practices for anyone:

- **Check your credit reports — for free — by visiting annualcreditreport.com:** Accounts or activity that you don't recognize could indicate identity theft. Visit IdentityTheft.gov to find out what to do.
- **Place a fraud alert on your credit file:** Once you place a fraud alert with one bureau, they will alert the other two.[2]
- **Place authentication features on financial accounts**: Ask your bank to require a password or pin to complete account transactions. Often fraudsters will call financial institutions to try to wire transfer funds, order new cards or change your address.
- **DMV alerts**: Next time you visit the DMV, you can ask if they can place a fraud alert on your driving record.
- **Set up an account at ssa.gov/myaccount:** Setting up an account with the Social Security Administration allows you to monitor your annual earnings to ensure a fraudster is not using your SSN for employment purposes. Setting up the account also ensures a fraudster doesn't set up the account to gain further access to your information.
- **Security Freeze:** Placing a Security Freeze with the credit bureaus locks your credit, making it inaccessible to creditors. When you place a Security Freeze, the bureaus will send you a confirmation pin number that will be used to lift your freeze. We recommend only lifting the freeze temporarily when you need to use your credit. You can remove the freeze on the credit bureaus' websites.
- **File an IRS Affidavit:** Alert the IRS of your compromised information by filling out the IRS Affidavit
- **Chex Systems Alerts:** You can place an alert with chexsystems.com to alert banks and financial institutions of your compromised information. This will help keep fraudsters from opening bank accounts in your name.

Together, all the way.®

Cigna®

- **Change all your passwords regularly:** Smart account management should include complex passwords that are changed regularly. Consider making your passwords on any financial accounts different than your email passwords, and make them as intricate as possible by including letters, numbers and symbols. Place authentication features such as passwords and pins that are required to complete such actions as address changes, account updates, wire transfers or ordering new cards.

- **Beware of phishing emails:** Once fraudsters gather identifying information, they usually send official-looking texts, emails or phone calls to gather more data. If you click on a link or respond to a text from an unfamiliar source, it may allow the fraudster to implant malware or viruses on your phone or computer. Never click on any links in emails or respond to unknown senders of text messages. If you receive something of concern that looks official, go to that business's secure website to get the correct phone numbers to call and inquire about messages you have received.

- **Beware of phone scams:** If you receive a call from a bill collector or other source soliciting you for money on a past due bill, you need to validate the debt. A recent scam involved fraudsters pretending to be the IRS and collecting thousands of dollars from victims that had their personal data compromised. Always confirm debts with creditors directly and remember that most of the time you should receive a letter in the mail before a phone call.

To learn more about the benefits and services available to you, contact your Employee Assistance Program at: 877.622.4327

Sources:

[1] New York Times, Equifax Says Cyberattack May Have Affected 143 Million in the U.S., September 7, 2017; https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?mcubz=0

[2] Equifax Alerts Online. https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp