Somerset Trust COMPANY
Member FDIC

Fraud News

What can happen after your Identity is Stolen?

So, you found out you may be a victim of a data breach. Perhaps you are one of the 143+ million people who had your identity stolen in the Equifax breach. Maybe you accidently allowed a Tech Support company remote access into your computer that you keep tax documents on. You may have even been notified by your Insurance Provider or Payroll Company that their systems were hacked. What do you do? Place a fraud alert or credit freeze on your credit report? Sure…that's a good place to start to help prevent credit or loan accounts from being opened in your name, but it's not going to keep you 100% safe from identity theft and the fraud that is associated with it. What else can fraudsters do with your identity information besides applying for credit cards and loans in your name? Keep reading to find out!

Drivers License Fraud- If a company (like Equifax), your doctor's office, or maybe even your local scrap yard is hacked, crooks may gain access to your driver's license information. Many times, they use this to apply for loans or credit cards but hopefully the fraud alert or credit freeze you placed will help with that. Fraudsters can also use a counterfeit driver's license along with a stolen SSN to open deposit accounts at banks, which normally do not pull credit history before opening an account. Shortly after the account is opened, the fraudster overdraws it and the collections process begins. There's a good chance that you will not know the account was opened until you start receiving collection notices, or you attempt to open a new deposit account and don't pass Qualifile screening! If the fraudsters create a counterfeit ID, they may use it along with the fraudulent bank account to write checks to different merchants (like Giant Eagle or Walmart). Once the checks begin to bounce or companies like Telecheck suspect fraudulent activity related to your identity, they will begin to refuse checks. If the day comes where you need to write a check at a merchant, you may be declined by Telecheck and have to start the recovery process to clear your name. Occasionally fraudsters may even try to present a fake driver's license at a traffic stop. If your ID passes the security checks and their tickets go unpaid, a warrant might be issued for your arrest! These types of fraudulent activity related to driver's license info are beginning to occur more and more, as they are difficult to detect by the victim. Counterfeit Drivers licenses sell on the dark web starting at $50 each and the more realistic ones (which duplicate holograms, mag stripes and chips) go for even more.

Fraudulent Tax Refunds- To some people, tax return (refund) time is the most wonderful time of the year! To others, it turns out to be a nightmare after they discover someone already submitted a tax return in their name. Not only is your refund delayed (In some cases, it has taken a year or more to resolve) but the hours you will spend on hold with the IRS will not do any good for your stress levels! Minimize risk of tax return fraud by filing early. You may also want to consider adjusting your withholding to more closely reflect your actual tax liability. You won't receive a large tax refund every spring but you will avoid some of the hassle if someone does file a fraudulent return in your name.

Medical/Insurance Fraud- If a fraudster gains access to your personal information or insurance information, they can receive medical treatment in your name. They may even use your information to receive prescription drugs (along with a counterfeit driver's license, of course!) You may start to receive bills from various doctors to pay down your deductible. Believe it or not, many people don't look at these bills very closely and what services were actually performed. There is an even more dangerous risk if someone starts receiving medical treatment in your name though…what happens if you need emergency medical treatment? Maybe you get into an accident or have a medical emergency while on

(Continued on next page…)

EQUAL HOUSING LENDER

vacation? If you are unable to give your medical history or provide a list of current medications, the doctors may have to obtain your medical records or information from other hospitals, PCP's or insurance companies. If someone else is using your medical/insurance information, you may end up being treated according to their medical history, drug allergies and current medications. In another extreme case, a woman had her medical ID stolen and the fraudster gave birth to a baby with drugs in her system. CPS notified her because they planned to place the baby in protective custody and possibly charge her with a crime. The only evidence that cleared her name was a DNA test that proved she was not the mother of the baby! To keep track of your medical records, make sure you read your Explanation of Benefits, look closely at any bills you receive, and contact your insurance company if you have any questions or see something you aren't sure belongs to you!

Becoming a target for other types of fraud- Once fraudsters have your personal identifying information, they may target you in an attempt to gain further access. Ironically, you may start receiving phishing calls or emails that offer to help you monitor your credit or protect your identity, and the catch is they will charge you an outrageous fee to do so. If you take the bait and enroll in their "services" you may give out your debit/credit card or bank account number which gives the fraudsters access to another layer of your identity.

They may also try to hack into your email account and send phishing emails or virus filled links to your friends and family. They may even use your social media accounts in an attempt to scam your friends and family out of money.

Conclusion- While most people think checking your credit report is the only thing they need to do after you place your fraud alert or credit freeze, there is really so much more that can be done to protect yourself and your identity!

- Read your mail, don't just assume it is all junk.
- Notify your bank or creditors right away if you notice your aren't receiving regular statements.
- Purchase and use reputable antivirus/malware programs. Your personal computer and or mobile devices can house a lot of your sensitive personal and financial information if you use it for anything more than just a place to login to Facebook or look at YouTube videos when you get bored.
- File a police report upon finding out your identity is being used fraudulently. In some cases, this may be the only way to clear your name!

For more information and resources go to identitytheft.gov.

Fraud Alert Reminder

It will soon be 90 days since news of the Equifax Breach broke.

- If you placed a **Fraud Alert** on your credit report, you need to renew it every 90 days. It may be helpful to set a reminder on your phone or calendar so you don't forget! You will only need to renew with one of the credit bureaus, they are required to update the other two. Be sure to remind friends and family to update these as well!
- A **Credit Freeze** stays on until you remove them. Just be sure to check that you placed one with each of the three credit bureaus (there is a fee from each Bureau to place these).