15 Business Center Drive
Swanzey, NH 03446

straight answers + bright solutions

TRUE NORTH NETWORKS

SECURE WORKPLACE®

With all the news lately about the security breach of Equifax, which has given thieves access to the data of more than 143 million people, we want to send our clients helpful information on how best to protect yourselves and your clients as a result of this event. We have followed the situation closely and reviewed many security bulletins so we could be informed of what took place, how Equifax is remediating the breach, and want to offer you our best advice on what steps you should take next. What follows is a bit lengthy, but every item I considered cutting for the sake of length was just too important to leave out. We want you to have as much information as possible so you can make informed choices.

Before we jump into the steps we want to clarify that normally, our advice would be to go directly to the vendor's breach information website for detailed information. In this case we don't recommend that for several reasons as noted below.

- Calling Equifax directly is ineffective right now. Operators handling phone calls don't have any further information about who was or was not affected in the breach.
- The Equifax breach notification website runs on a stock installation of WordPress. This is cause for concern as it appears to have insufficient security for a site that asks people to provide their last name plus six out of nine digits of their Social Security number. If this information was stolen, it would be more than enough fodder for criminals to perpetrate additional fraud.
- Software with phishing-detection functionality such as OpenDNS have been blocking access to the site and warning that it was a suspected phishing threat due to irregularities in its functionality. For example, the SSL/TLS certificate doesn't perform proper revocation checks, which may cause browsers to display an error message. And the domain name is registered to a site that is not clearly labeled as belonging to Equifax.
- Many reports indicate that the information coming out of the website database check (to determine if you were affected) may be incomplete or altogether inaccurate.
- Signing up for TrustID's credit monitoring service is provided by Equifax, the same company that was breached in the first place and if not cancelled after the one year free period, monthly charges will incur. There was also some verbiage that initially indicated that signing up for the credit monitoring product would forfeit your right to join a class action suit against Equifax in relation to the breach. That statement has since been clarified that it does not prohibit consumers from taking legal action.

Indications are that this breach occurred between mid-May and July 2017, and that it was discovered by Equifax on July 29. As this has potentially affected almost half of all adults in the US, you may be wondering how to identify or mitigate problems caused by this breach.

Here are a few steps you can take now:

15 Business Center Drive
Swanzey, NH 03446
straight answers + bright solutions

TRUE NORTH NETWORKS

SECURE WORKPLACE®

1. Check your accounts for suspicious activity

The first, and most important thing you can do is to check the transactions on all your financial accounts and credit history. Keep in mind that there is an overwhelming amount of traffic going to all the major credit reporting agencies right now, so they may be slow or only intermittently available for the next few days. As the breach was only recently reported, it's likely that more information about the specifics of who was affected and what was stolen will become available in the coming days and weeks.

If you see activity that you do not recognize, it is important that you notify the bank or credit agency immediately.

The data stolen includes names, social security numbers, birth dates, addresses, and the numbers of some driver's licenses and credit cards. Keep in mind that the thieves may not use or sell all of the stolen data right away. You will need to be vigilant with your accounts for a while, possibly even for years to come.

2. Consider a Credit Freeze

While freezing your credit does introduce an obstacle when it comes to allowing someone to access your credit report (such as when you apply for a new bank card, loan, apartment or job), it also makes it more difficult for thieves to create new accounts using your information. Laws differ from one state to another regarding who may request a freeze and how much they will be charged. For most states that do charge, if fraud against you has not yet been committed as the result of a data breach, you may be charged around $10 to place the freeze. It's important to contact all three credit reporting agencies, including Equifax.

If your information was included in this breach, and you decide against a credit freeze, you may wish to place a fraud alert on your files instead. A fraud alert warns creditors that you may be a victim of identity theft and that they should take additional steps to verify that anyone seeking credit in your name really is you.

An Initial Fraud Alert lasts 90 days, which won't be very helpful in this case as criminals can and most likely will be (mis)using permanent credentials like Social Security Numbers for years to come. To file an Extended Fraud Alert that lasts seven years, you must have a police report that describes identity theft-related fraud that has already been perpetrated against you.

3. File your taxes promptly

While thieves may use stolen information to create fraudulent bank accounts, they may also use it to file fraudulent tax returns. File your taxes as soon as you have the tax information you need and respond promptly to letters sent to you by the IRS. Note that the IRS will never communicate with you via email, so watch out for this type of fraud and don't open emails purporting to be from the IRS.

15 Business Center Drive
Swanzey, NH 03446
straight answers + bright solutions

TRUE NORTH NETWORKS

SECURE WORKPLACE®

4. Improve your login security

With all the information that is now available to thieves, they may try to combine it with attacks on other online accounts and services. It's always a good idea to make sure you have strong, unique passwords for each account you use. If you've not yet enabled two-factor authentication wherever it's available to you, now is a great time to make sure you have this in place.

5. Beware of scams

Criminals are aware that people will be feeling especially anxious about their security and privacy as a result of this incident. This could lead to other scams and has already inspired at least one phishing site passing itself off as an Equifax resource. Some people may, ironically, be more apt to fall for social engineering tactics and phishing schemes that prey on this fear. Never click on links in emails purporting to come from businesses using this angle, especially if they appear suspicious in any way. It's a good idea, especially after major security events and other crises, to consider any link in an unsolicited email to be potentially malicious. Instead, you should type URLs that you know to be genuine into your browser directly if you need to contact companies.

There are plenty of things you can do to protect yourself without needing to contact Equifax right now. Equifax will contact affected consumers directly by mail, so for now, keep an eye on the news as more information comes to light.

I have included a useful list of websites where you can find additional information about placing a credit freeze, fraud alert, etc.

How to freeze your credit –

https://help.equifax.com/s/article/ka137000000DSDjAAO/How-do-I-place-a-security-freeze-on-my-Equifax-credit-file

http://www.ncsl.org/research/financial-services-and-commerce/consumer-report-security-freeze-state-

statutes.aspx

http://www.creditreporting.com/innovis.html

http://www.atg.wa.gov/security-freeze-procedures

How to place a fraud alert –

https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs#difference

http://www.kiplinger.com/article/credit/T017-C001-S001-fraud-alert-vs-credit-freeze.html

Additional read with great Q&A –

https://krebsonsecurity.com/2017/09/the-equifax-breach-what-you-should-know/

Sources –

https://www.helpnetsecurity.com/2017/09/11/equifax-failed-miserably/

https://www.welivesecurity.com/2017/09/11/equifax-breach-5-defensive-steps/