EQUIFAX

A devastating cyberattack on Equifax compromised critically sensitive information.

Equifax said a cyberattack exploited an exposure in their website software that impacted 143 million consumers. The hackers also gained access to files containing names, Social Security numbers, birth dates, addresses and driver's license numbers. In addition, the hackers took credit card numbers for about 209,000 consumers as well as "dispute" documents for about 182,000 consumers. Finally, Equifax said the breach also impacted an undisclosed number of people in Canada and England.

Equifax said **t**he breach was open from mid-May to July 29. On September 7, forty-one (41) days later, it reported the breach.

After Equifax revealed the cyberattack, thousands logged onto the Equifax website to see if they were at risk. For many, the site did not work at first. But for those who got through, an unpleasant surprise was waiting.

Equifax offered a free year of credit monitoring known as "TrustedID Premier" if the consumer's data was indeed stolen. But in the fine print, consumers found that by agreeing to the service, they would give up the right to sue over damages related to the attack. If they wanted to recover damages they would have to go an arbitration process set up by Equifax. Lawmakers jumped into the fray and social media flooded the airwaves with messages of concern, worried that the private proceeding was inherently biased in favor of Equifax. After a day of harsh criticism, Equifax said consumers would not have to give up their right to pursue class action lawsuits related to damages stemming from the incident.

> Sept. 10: Equifax issues a new statement further clarifying its stance on the arbitration clause. *"To confirm, enrolling in the free credit file monitoring and identity theft protection products that we are offering as part of this cybersecurity incident does not prohibit consumers from taking legal action."*
>
> *Again," Equifax continued, "to be as clear as possible, we will not apply any arbitration clause or class action waiver against consumers for claims related to the free products offered in response to the cybersecurity incident or for claims related to the cybersecurity incident itself."*
>
> *The company said it removed the arbitration language from the terms of use on its data breach notification site, equifaxsecurity2017.com. It also said that the terms of use on Equifax's main site, equifax.com, do not cover the TrustedID Premier service, which has its own terms of use.*

Was this just thoughtless mistake, confusion over what to put out, or can I get away with it?

Initially, Equifax included a mandatory arbitration clause in the fine print of its free credit-monitoring product offered in the wake of the cyberattack. This would prevent consumer who opted for the product from being able to sue. Consumer only found this caveat if they read through a painstakingly long legalese agreement (i.e., written for lawyers, not consumers).

Customers, social media, and Congress (almost) immediately cried foul (it took a lit bit of time and a second or third read of the agreement). However, as the roar grew, Equifax removed the clause.

Conclusion: just as Equifax chose not to spend money on cyber security, it initially chose to do as little as possible to help those aggrieved by the hack.

This is no ordinary breach; it cannot be fixed by issuing a new credit card and blocking the bad credit card that was compromised! We actually will not know the full repercussions of this intrusion for years.

The Federal Trade Commission (FTC), which oversees data protection, cannot (by law) dispense **large** financial fines for transgressions. The FTC's main focus is on the accuracy of data and the products that are sold to

consumers. More troubling, most expect that even though this is a massive problem for consumers, Congress will probably not act—it has too many other headline issues before it.

Consumer advocates have been pressing for stricter oversight of the credit bureaus and stronger privacy rules covering all companies for years. This is the type of breach many were afraid would happen. Additionally, the Consumer Financial Protection Bureau has found that the credit bureaus lack sufficient quality controls to make sure consumers' data is accurate and secure. Finally, Senator William Proxmire **in 1969** said, "credit bureaus are almost entirely responsive to the needs of business and have little responsibility to consumers; it is difficult to see major expenditures on security systems in the absence of public standards." As a fitting conclusion, Equifax has been a powerful force in the legislative and regulatory arena, spending over a million dollars last year on lobbying for less regulation, not more.

So what can you do; follow these five steps if they you are worried:

1. Check your free credit reports
   You can request a free copy of your credit report, at www.annualcreditreport.com, once a year from each of the three credit reporting agencies: Equifax, Experian, and TransUnion.
2. Put a fraud alert on your credit
   You can put a fraud alert on your credit reports for free by contacting **one** of the credit agencies, which is required to notify the other two. This means you'll be contacted if someone tries to apply for credit in your name. It will last for 90 days and can be renewed.
3. Open and review your monthly bank account and credit card statements along with your retirement and brokerage account statements.

   Look for any suspicious activity. Theft typically happens over time. It may start small (unnoticeable) but it can lead to money being stolen from all your accounts. Develop the habit of carefully checking your statements on a regular basis.
4. Sign up for a credit monitoring or identity theft protection service

   Most credit monitoring services alert you when a company checks your credit history or when a new loan or credit card is opened in your name, or if a creditor says a payment is late. However, since most services only track credit reports, they will not alert you to suspicious activity on your credit card or bank accounts.

   Some monitoring services include identity theft protection, which alerts you when your personal information is being used in ways that do not show up on your credit report. These services won't prevent fraud from happening. Some offer identity recovery services to help you regain control of your finances after identity theft occurs. The government offers a free resource for recovering from identity theft at IdentityTheft.gov.

   While there is usually a cost involved with a credit monitoring service or identity theft protection, Equifax is offering a free year of credit monitoring through its TrustedID Premier business. This will track your credit report from Equifax, as well as your reports from the two other credit reporting agencies, and alert you to certain changes. TrustedID Premier will also provide free copies of those reports and the ability to lock your Equifax credit report so companies cannot see it.
5. Put a freeze on your credit
   A freeze blocks anyone from accessing your credit reports without your permission. But it can be an inconvenience for you, too. If you want to take out a loan or open a new credit card, you'll have to contact the reporting agency to temporarily lift the freeze. It's also not free. Fees to freeze and unfreeze your account vary by state, but commonly range from $5 to $10 for each.

   For more information on Equifax cyberattack, see BEFCU's website.

While Equifax is a huge problem, members are cautioned not forget that cyber thieves work in many different arenas. Members need to stay on top of their information to ensure that they do not become a victim of a scam, fraud or identify theft.

Beware of phishing emails. Phishing is when a scammer uses fraudulent emails or texts, or copycat websites to get you to share valuable personal information – such as account numbers, Social Security numbers, or your login IDs and passwords. Scammers use your information to steal your money or your identity or both.

Scammers use phishing emails to get access to your computer or network then they install programs like ransomware that can lock you out of important files on your computer.

Scammers lure targets (you or other members) into a false sense of security by spoofing the familiar, trusted logos of established, legitimate companies. Or they pretend to be a friend or family member.

Scammers make it seem like they need your information or someone else's, quickly–sometimes they make you think something bad will happen unless you comply. They might say your account will be frozen, you will fail to get a tax refund, or you could be arrested. They will lie to get you to give them information.

Make the call if you're not sure. Do not respond to any emails that request personal or financial information. Phishers use pressure tactics and prey on fear. If you think a company, friend or family member really does need personal information from you, pick up the phone and call them yourself using the number on their website or in your address book, not the one in the email.

Be cautious about opening attachments or clicking on links in emails, even if it is from a friend or family member. Files and links can contain malware that can penetrate your computer's security.

Do your own typing. If a company or organization you know sends you a link or phone number, don't click. Use your favorite search engine to look up the website or phone number yourself. Even though a link or phone number in an email may look like the real deal, scammers can hide the true destination.

Turn on two-factor authentication. For accounts that support it, two-factor authentication requires both your password and an additional piece of information to log in to your account. The second piece could be a code sent to your phone, or a random number generated by an app or a token. This protects your account even if your password is compromised.

As an extra precaution, you may want to choose more than one type of second authentication (e.g. a PIN) in case your primary method (such as a phone) is unavailable.

Back up your files to an external hard drive or cloud storage. Back up your files regularly to protect yourself against viruses or a ransomware attack.

Keep your security up to date. Use security software you trust, and make sure you set it to update automatically.

Report phishing emails and texts.

1. Forward phishing emails to spam@uce.gov –if the organization is legitimate, send it to the organization impersonated in the email.

   This is the Federal Trade Commission's (FTC) email box: spam@uce.gov; this is where consumers send unwanted or deceptive spam to the FTC.

   File a report with the Federal Trade Commission at FTC.gov/complaint.

2. Visit Identitytheft.gov. Victims of phishing could become victims of identity theft; there are steps you can take to minimize your risk.

   IdentityTheft.gov is the federal government's one-stop resource for identity theft victims. The site provides checklists and sample letters to guide you through the recovery process.

Some additional information related to the breach and to Equifax:

Q: What is a security freeze?

A: A security freeze essentially blocks any potential creditors from being able to view or "pull" your credit file, unless you affirmatively unfreeze or thaw your file beforehand. With a freeze in place on your credit file, it will be very hard for thieves to get new lines of credit in your name.

Q: What's involved in freezing my credit file?

A: Freezing your credit involves notifying each of the major credit bureaus that you wish to place a freeze on your credit file. This can usually be done online, but in a few cases you may need to contact one or more credit bureaus by phone or in writing. Once you complete the application process, each bureau will provide a unique personal identification number (PIN) that you can use to unfreeze or "thaw" your credit file in the event that you need to apply for new lines of credit sometime in the future. Depending on your state of residence and your circumstances, you may also have to pay a small fee to place a freeze at each bureau. There are four consumer credit bureaus, including Equifax, Experian, Innovis and Trans Union.

Q: How much is the fee, and how can I know whether I have to pay it?

A: Fees range from $0 to $10 per bureau, meaning that it could cost up of $60 to place a freeze at all four credit bureaus. However, in most states, consumers can freeze their credit file for free at each of the major credit bureaus if they can supply a copy of a police report and in some cases an affidavit stating that the filer believes he/she is or is likely to be the victim of identity theft. In many states, that police report can be filed and obtained online. The fee covers a freeze as long as the consumer keeps it in place.

Q: What's involved in unfreezing my file?

A: The easiest way to unfreeze your file for the purposes of gaining new credit is to spend a few minutes on the phone with the company from which you hope to gain the line of credit (or perhaps research the matter online) to see which credit bureau they rely upon for credit checks. It will most likely be one of the major bureaus. Once you know which bureau the creditor uses, contact that bureau either via phone or online and supply the PIN they gave you when you froze your credit file with them. The thawing process should not take more than 24 hours.

What's the difference between a security freeze and a fraud alert on my credit file?

A: With a fraud alert on your credit file, lenders or service providers should not grant credit in your name without first contacting you to obtain your approval — by phone or whatever other method you specify when you apply for the fraud alert. To place a fraud alert, contact one of the credit bureaus via phone or online, fill out a form, and answer a handful of multiple-choice, out-of-wallet questions about your credit history. Assuming the application goes through, the bureau you filed the alert with must by law share that alert with the other bureaus. Fraud alerts only last for 90 days, although you can renew them as often as you like.

Consumers also can get an **extended fraud alert**, which remains on your credit report for seven years. An extended fraud alert requires a police report or other official record showing that you've been the victim of identity theft.

An **active duty alert** is another alert available if you are on active military duty. The active duty alert is similar to an initial fraud alert except that it lasts 12 months and your name is removed from pre-approved firm offers of credit or insurance (prescreening) for 2 years.

Q: Why would I pay for a security freeze when a fraud alert is free?

A: *While lenders and service providers are supposed to seek and obtain your approval before granting credit in your name if you have a fraud alert on your file, they're not legally required to do this.*