Equifax Cybersecurity Incident

What happened?

- On September 7, 2017, Equifax announced that files containing personal information relating to 143 million customers were accessed without authorization from May 13 through July 30, 2017.
- Equifax believes that the breach occurred through a vulnerability in Apache Struts, an open-source application framework that supports the Equifax online dispute portal web application. The vulnerability was patched on July 30, 2017.

What personal information may have been exposed?

- Names, Social Security numbers, birth dates, addresses, and, in some instances, driver's license numbers
- Credit card numbers for approximately 209,000 customers
- Dispute documents with personal identifying information for approximately 182,000 customers

How do I tell if I am affected?

- To determine if your personal information is impacted, visit https://www.equifaxsecurity2017.com/potential-impact/ or call **866-447-7559** any day (including weekends) between 7:00 am and 1:00 am Eastern time.
- The site requires your last name and the last six digits of your Social Security number so make sure you're on a secure computer and an encrypted network connection any time you enter it.

What is Equifax doing in response?

- Regardless of whether you have been impacted, Equifax is offering free credit file monitoring and identity theft protection for one year to all U.S. customers through TrustedID Premier. Visit https://equifaxsecurity2017.com/enroll/ to begin enrollment.
- TrustedID Premier includes 3-Bureau credit monitoring of Equifax, Experian, and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers.
- Arbitration and class-action waiver clauses initially included in the Terms of Use have been removed and will not apply to customers who enrolled before the language was removed.
- No credit card information is required to sign up and customers will not be automatically charged after the conclusion of the complimentary year.
- You have until November 21, 2017 to enroll in TrustedID Premier.

What can I do to protect my information?

- Check your credit reports from Equifax, Experian, and TransUnion for free by visiting https://www.annualcreditreport.com. Pay attention to accounts or activity that you do not recognize as those could indicate identity theft.
- Monitor your existing credit cards and bank accounts closely and let your financial providers know of any unfamiliar charges as soon as you become aware of them.
- File your taxes as soon as you have the tax information you need. Tax identity theft occurs when someone uses your Social Security number to get a tax refund.
- Consider placing a fraud alert or credit freeze on your files.

What is the difference between a fraud alert and a credit freeze?

- With a fraud alert, a business must try to verify a customer's identity before extending new credit. Usually that means calling to check if the person is actually at the particular establishment attempting to obtain credit. Fraud alerts may be effective at preventing someone from opening new credit accounts in your name, but they may not prevent the misuse of your existing accounts.
- With a credit freeze, no one – including the consumer – can access the consumer's credit report to open a new account. If consumers put a credit freeze in place, they'll receive a PIN number to use each time they want to freeze, unfreeze, and refreeze their account.

When should I place an Initial Fraud Alert?

- If you are concerned about identity theft, but are not yet a victim, placing a fraud alert may protect your credit from unverified access.
- An Initial Fraud Alert lasts 90 days. After 90 days, you can renew the fraud alert.
- Placing an Initial Fraud Alert is free.
- To place an Initial Fraud Alert, contact one of the three credit reporting agencies and request that an Initial Fraud Alert be placed on your credit report. The agency you contact is required to notify the other two agencies.

When should I place an Extended Fraud Alert?

- If you are a victim of identity theft, consider creating an Identity Theft Report with the Federal Trade Commission. Visit https://www.identitytheft.gov for more information.
- After creating an Identity Theft Report, you can place an extended fraud alert on your credit file. When you place an extended alert, you can get 2 free credit reports within 12 months from each of the three nationwide credit reporting companies.
- An Extended Fraud Alert lasts for 7 years.
- Placing an Extended Fraud Alert is free.
- To place an Extended Fraud Alert, contact one of the three credit reporting agencies and request that an Extended Fraud Alert be placed on your credit report. The agency you contact is required to notify the other two agencies.

When should I place a Credit Freeze?

- If you are concerned about identity theft or someone gaining access to your credit report without your permission, consider placing a credit freeze on your report. A credit freeze makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account.
- After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN or password. You will need the PIN if you choose to lift the freeze.
- Keep in mind that activities such as applying for a job, renting an apartment, buying insurance, or opening a new account may be delayed by a Credit Freeze. In order for parties such as a landlord, employer, or financial institution to see your credit report, you will need to lift the freeze temporarily.
- Certain entities will have access to your credit report while it is frozen, including existing creditors, debt collectors, and government agencies acting in response to a court or administrative order, a subpoena, or a search warrant.
- In most states, a Credit Freeze remains in place until you request that it be lifted or removed. However, in a few states, a Credit Freeze expires after seven years.
- Placing a Credit Freeze may require a fee, which varies by state law.
    - In North Carolina, each agency may charge you up to $3.00 to place a freeze. Minors under the age of 16 may be charged up to $5.00 to place a freeze. If you are a victim of identity theft or are over the age of 62, placing a freeze is free.
    - In South Carolina, placing a freeze is free.
    - In Georgia, each agency may charge you up to $3.00 to place a freeze.
    - In Virginia, each agency may charge you up to $10.00 to place a freeze. If you are a victim of identity theft, placing a freeze is free.
- To place a Credit Freeze, contact all three credit reporting agencies.

	Initial Fraud Alert	Extended Fraud Alert	Credit Freeze
Description	Prevents access to your credit report	Prevents access to your credit report	Stops all access to your credit report
Duration	90 days	7 years	In most states, until you lift or remove the freeze
Cost	Free	Free	Up to $10
Consumer Requirements	None	Must be a victim of identity theft with an Identity Theft Report	None
Who to contact	One agency; law requires the agency notify the other two of the fraud alert request	One agency; law requires the agency notify the other two of the fraud alert request	Each agency independently
Contact Equifax	1-888-766-0008 OR begin at https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp	1-888-766-0008 OR complete the form at https://www.alerts.equifax.com/AutoFraud_Online/pdf/Fraud_Alert_7.pdf AND mail it to: **Equifax Information Services** PO Box 105069 Atlanta, GA 30348-5069	1-888-766-0008 OR begin at https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
Contact Experian	1-888-397-3742 OR begin at https://www.experian.com/ncaconline/fraudalert	1-888-397-3742 OR complete the form at https://www.experian.com/fraud/form-extended-fraud-victim-alert.html AND mail it to: **Experian** PO Box 9554 Allen, TX 75013	1-888-397-3742 OR begin at https://www.experian.com/ncaconline/freeze
Contact TransUnion	1-800-680-7289 OR begin at https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp	1-800-680-7289 OR complete the form at https://fraud.transunion.com/pdf/ExtendedAlertForm.pdf? AND mail it to: **TransUnion** PO Box 2000 Chester, PA 19016	1-888-909-8872 OR begin at https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp