LWC

LORING, WOLCOTT & COOLIDGE

Trusted Relationships *for* Generations

Equifax Data Breach

On September 7, 2017, Equifax announced what appears to be the largest breach of consumer data in US history. You should assume that your data, including your social security number, is almost certainly a part of this breach. Potential steps to consider:

1. Monitor Your Credit Reports

- You can hire a credit monitoring service such as IdentityForce, LifeLock, IDShield, Identity Guard, or Credit Secure (or a number of other companies including Equifax's free one-year offer).
- Request a free credit report at: https://www.annualcreditreport.com or call 877-322-8228.
- This doesn't prevent identify theft, but enables you to act if you see fraudulent activity.
- Monitor you bank accounts and credit cards.

2. Consider Placing a Credit Freeze (also known as a Security Freeze)

- A credit freeze restricts access to your credit report and makes it difficult for thieves to open accounts in your name.
- A credit freeze won't prevent a thief from accessing your existing accounts. It is intended to stop the fraudulent opening of any new credit using your identifying information.
- Credit freezes can be placed with each of the major credit bureaus (and one small one) as follows:
  - **Experian:** 888-397-3742 or https://www.experian.com/freeze/center.html
  - **Transunion:** 888-909-8872 https://www.transunion.com/credit-freeze/place-credit-freeze2
  - **Equifax**: 800-349-9960 or https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
  - **Innovis**: 800-540-2505 or https://www.innovis.com/personal/securityFreeze

  There may be a small fee for placing a freeze on your account and the freeze will have to be removed before applying for credit (mortgage, HELOC, credit card, etc.).
  IMPORTANT: Don't lose your PIN or leave it open to theft by third parties

3. Fraud Alert

- Place a fraud alert with each of the credit rating agencies. A fraud alert is intended to warn creditors that you may have been the victim of identity theft and asks them to verify the identity of anyone seeking credit in your name. Fraud alerts can be placed using the following links:
  - **Experian:** https://www.experian.com/fraud/center.html
  - **Transunion:** https://www.transunion.com/fraud-victim-resource/place-fraud-alert
  - **Equifax**: https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
  - **Innovis:** https://www.innovis.com/personal/fraudActiveDutyAlerts

4. Two-Step Verification

- Whenever offered, activate two-step verification for all websites and email accounts. Typically, in addition to regular on-line login information, websites will require another form of authentication through a code, usually in a text message, which you enter as the final login step, thereby adding an extra layer of security.

For additional information, please see FTC's Identity Theft website at: https://identitytheft.gov/Steps