CLIFFORD SWAN

INVESTMENT COUNSELORS

CYBERSECURITY BREACHES

You discovered that your personal information or account has been compromised.

What do you do next?

Contact Clifford Swan Investment Counselors so we can watch for any suspicious activity in your accounts and collaborate with you on extra precautions to take in verifying your identity prior to any fund transfers.

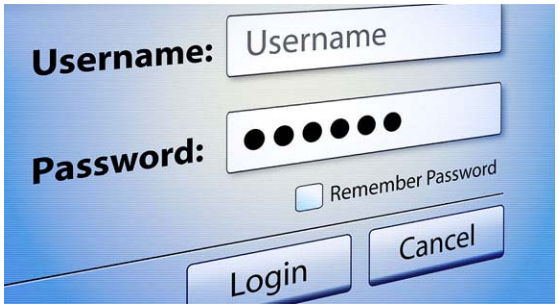
We have identified key areas in which data breaches frequently occur and have outlined a few steps to assist you with resolving each type of breach.

Social Security Number

- Call the Social Security Administration's fraud hotline at 800-269-0271 if you suspect your Social Security number has been compromised. The Office of the Inspector General will take your report and investigate activity using your Social Security number.
- Contact the Federal Trade Commission (FTC), either at www.identitytheft.gov, by calling 1-877-IDTHEFT, or by visiting www.ftc.gov. Click on "Report Identity Theft" to access the Identity Theft Recovery Steps. This one-stop resource for victims of identity theft will guide you through each step of the recovery process, from reporting the crime to creating a personal recovery plan and putting your plan to action.
- Get free credit reports from http://www.annualcreditreport.com. Check for any accounts or charges you don't recognize.
- If a company responsible for exposing your personal information offers you free credit monitoring, take advantage of it. If not, consider using your own credit/identity monitoring service.
- Consider placing a credit freeze with the major credit bureaus (Equifax, Experian, TransUnion) to prevent your information from being exploited. If you place a freeze, be ready to take a few extra steps the next time you apply for a new credit card or cell phone – or any service that requires a credit check.

  Phone: 800-349-9960 https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
  Phone: 888-397-3742 https://www.experian.com/freeze/center.html
  Phone: 888-909-8872 https://www.transunion.com/credit-freeze/place-credit-freeze

- If you decide not to place a credit freeze, at least consider placing a fraud alert.
- Continue to monitor your credit reports on an ongoing basis.



Online Accounts & Email:

- Run reputable anti-virus/anti-malware/anti-spyware software to clean your computer.
- Once you've ensured your computer is virus/malware/spyware free, you should change your login password. Make each password unique and complex, and use two-factor authentication when available.
    - Don't use simple dictionary words
    - Use passwords that are at least 20 characters long (8 character passwords can be cracked in about 6 hours)
    - Use a "pass phrase" instead of a password (Ex: "threedollarsforthepiratehat")
    - Use a different password for each website and don't use patterns
    - Change passwords every 60-90 days
- If possible, also change your username. If you can't log in, contact the company and ask them how you can recover or shut down the account.
- If you use the same password anywhere else, change that, too.
- Change your security questions and answers.
    - Make sure your security question answers are as hard to guess as your password (Don't use standard answers such as maiden names, birthplaces, etc. The answers to most of those questions are easily found online).
- Notify your friends, family, business associates, and other relevant parties in your contact list that you were hacked. Tell them to beware of emails that may have been sent to them from your account.

Bank Account / Credit Card Information:

- Contact your bank to close the account and open a new one. Contact your credit card company to cancel your card and request a new one.
- Place a fraud alert on your accounts with the major credit bureaus (Equifax, Experian, TransUnion)
  - Phone: 888-766-0008 https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
  - Phone: 888-397-3742 https://www.experian.com/fraud/center.html
  - Phone: 888-909-8872 https://www.transunion.com/fraud-victim-resource/place-fraud-alert
- If you log in to your bank account or credit card account online, you should change your login password. If possible, also change your username. If you can't log in, contact the bank or credit card company. Ask them how you can recover or shut down the account.
- If you use the same password anywhere else, change that, too.
- Review all recent account statements for unauthorized activity and report any suspicious transactions. If you find fraudulent charges or withdrawals, call the fraud department to get them removed.
- If you have automatic payments set up, update them with your new bank account information.
- If your credit card or bank account is linked to any online retail stores or bill pay sites, go through each account and remove linked information as soon as possible so that any future purchases can only be made by manually entering the new credit card or bank account information.

Brokerage Account:

- Contact Clifford Swan to work with you, and your custodian to close any compromised or unauthorized accounts. A cloned account can be requested through the custodian. This allows an identical account to be opened, your assets moved, and the compromised account closed.
- If you log in to your brokerage account online, you should change your login password. If possible, also change your username. If you can't log in, contact the custodian. Ask them how you can recover or shut down the account.
- If you use the same password anywhere else, change that too.
- Review all recent account statements for unauthorized activity and report any suspicious transactions. *Clifford Swan Investment Counselors is committed to monitoring transfers and transactions within client accounts and seeking to authenticate clients and client requests for transfers, whether such requests direct the transfer of funds from the client's account to third party payees or to another account in the client's name, particularly (though not exclusively) when the receiving client account was only recently opened and/or the request was received via email or other electronic communication.*
- Add a verbal password on your account with your custodian. When this has been put in place, the password must be given to the service representative on the phone before they will discuss any account information.
- Consider using a security token if your custodian offers them.