COMPREHENSIVE
WEALTH MANAGEMENT

RESPONDING TO A DATA BREACH

A cybersecurity breach isn't a disaster, however mishandling it is.

Time is of the essence, whether your personal data has been compromised as part of a larger targeted cyberattack, or you are the victim of an individual cybercrime. You'll need to take immediate action to minimize the impacts.

Within the first 24-48 hours

Call your CWM advisor, regardless of where or how the breach occurred, so we can watch for any suspicious activity in your CWM managed accounts and collaborate with you on extra precautions to take in verifying your identity prior to any fund transfers or account updates. We will call Schwab on your behalf to restrict trading in the accounts until the issue is resolved.

Alert your bank, credit card company, and any other financial institutions of the breach. Add Multifactor Authentication to these accounts and sign up for activity alerts.

If you suspect your Social Security number has been compromised, **call the Social Security Administration's fraud hotline at (800) 269-0271.** The Office of the Inspector General will take your report and investigate activity of your SSN. Visit ssa.gov/fraud for more info.

Report identity theft with the Federal Trade Commission (FTC) by visiting www.IdentityTheft.gov or call (877) 438-4338. 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 and enacting a personal recovery plan.

Run reputable anti-virus / anti-malware / anti-spyware software to clean your computer of any installed malicious software.

Once your computer is virus / malware / spyware free, **update passwords on accounts such as email, financial institutions, and social media. Turn on Multifactor Authentication (MFA).** Follow this step even if the breach was not due to installed malware.

Comprehensive Wealth Management
3500 188th St. SW, Suite 102 | Lynnwood, WA 98037 | (425) 778-6160 | (800) 268-2440
www.CWMnw.com

Within the first 24-48 hours *(continuted)*

If you suspect you're a victim of identity theft, call Schwab's Identity Theft Hotline at (888) 372-4922. Schwab will investigate your case and take necessary precautions to prevent unauthorized debit. Schwab's Identity Theft team can answer questions, discuss how Schwab handles accounts of clients who've had their identity stolen or their account hacked, and **assist with enhanced authentication**.

If appropriate, **close any compromised or unauthorized accounts.**

Freeze your credit with each of the main credit bureaus to prevent the unauthorized opening of accounts. Executing a freeze with one credit bureau will *NOT* automatically update the others. You can easily unfreeze your credit report when needed.

Equifax	Experian	TransUnion
www.equifax.com	www.experian.com	www.transunion.com
(888) 298-0045	(888) 397-3742	(800) 916-8800

If the breach is associated with your email or social media accounts alert family, friends, and associates. Let them know not to click any links or to send money in response to recent messages from you.

Within the first week

If the breach occured at a firm with whom you do business, be sure to follow the legitimate directions provided by that firm. **If the firm offers, sign-up for credit protection services.**

Report the crime to your local police, even though the incident may cross multiple jurisdictions. The police will file a formal report and may be able to to refer you to resources and agencies that can provide additional support. Record the police report number.

Place a Fraud Alert with one of the three major credit bureaus. Provide the credit bureau with the police report number and ask them to place a fraud alert on your account to prevent additional fraudulent activity. Once the fraud alert is activated, the two other credit bureaus will be notified. The fraud alert on your credit report will remain active for seven years with all three credit bureaus. (Without the police report number, the alert will only last one year.)

Review all recent account statements for unauthorized activity and report any suspicious transactions to the business or organization where the activity occurred.

Collect and save evidence such as account statements, canceled checks, receipts, and emails that may be useful if an investigation is warranted regarding the cybercrime.