LVW ADVISORS

# RESPONDING TO A DATA BREACH

LVW ADVISORS
WWW.LVWADVISORS.COM

# RESPONDING TO A DATA BREACH

The cyber threat landscape continues to evolve with more sophisticated attack methods and a larger volume of hacking attempts. If your personal data has been compromised as part of a larger targeted cyberattack, or if you are the victim of an individual cybercrime, time is of the essence. You'll need to take immediate action to minimize the impacts. Here are steps you should take within specified timeframes after discovering your data has been breached.

## WITHIN 24-48 HOURS

- Call LVW so your advisor 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.

- Notify custodians, banks, and other financial institutions so they can investigate your account activity and take necessary precautions to prevent further unauthorized debits. If appropriate, close any compromised or unauthorized accounts. Alternatively, you may be able to request a cloned account, which allows an identical account to be opened, your assets moved, and the compromised account closed.

- Run reputable anti-virus/anti-malware/anti-spyware software to clean your computer.

- Once you've ensured your computer is virus/malware/spyware free, change passwords on your accounts. Make each password unique, long, and strong, and use two-factor authentication when available.

- Contact government agencies that will investigate fraudulent activity and assist you with recovery.

## FEDERAL TRADE COMMISSION

**1-877-IDTHEFT (TTY 1-866-653-4261); www.identitytheft.gov; 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.

## SOCIAL SECURITY ADMINISTRATION

**800-269-0271**
The Office of the Inspector General will take your report and investigate activity using your Social Security number. You can also create an online Social Security account, which will enable you to access and review your statement online and verify its accuracy.

## INTERNAL REVENUE SERVICE

**https://www.irs.gov/uac/taxpayer-guide-to-identity-theft**
You'll be able to access the Taxpayer Guide to Identity Theft, which provides education on tax-related identity theft, tips to reduce your risk, and steps for victims to take.

## WITHIN 1 WEEK

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

- Report the crime to your local police, even though the incident may cross multiple jurisdictions. Your local police will file a formal report and may be able to refer you to additional resources and agencies that can help.

- Report your stolen money and/or identity to one of the three main credit bureaus. Provide the credit bureau with your 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 receive automatic notification and the fraud alert on your credit report will be in place for seven years with all three credit bureaus. (Without a police report number, the alert will only be in place for 90 days.)

### CREDIT BUREAU CONTACT INFORMATION:

Equifax 1-800-525-6285 | www.freeze.equifax.com

Experian 1-888-397-3742 | www.experian.com/freeze/center.html

TransUnion 1-800-680-7289 | www.transunion.com/securityfreeze

## WITHIN 1 WEEK(CONTINUED)

- Put a freeze on your credit report 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.

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

- Consider what other personal information (e.g., birth date, social security number, PIN numbers, account numbers and passwords) may be at risk and alert the appropriate businesses.

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

## THE NEXT 30 DAYS AND BEYOND

- Carefully review statements on all accounts as soon as they arrive. Look for unauthorized activity and report any suspicious transactions to the business where the unauthorized or suspicious activity occurred.

- 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.

- Request a credit report every six months to check for unauthorized activity. It will NOT affect your credit score.

# AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE

**Take these steps to secure your online presence:**

- ☑ Shred documents with private information that are no longer needed.
- ☑ Update your computer settings to install updates automatically.
- ☑ Windows and Apple computers have firewalls, anti-virus, and anti-spyware baked into them. Make sure they are turned on.
- ☑ Always log out. Don't use public computers. Instead of using public wifi (for instance at a Starbucks), use your phone as a mobile hotspot.
- ☑ Practice browser safety. Don't auto store passwords, look for "https" in website address, and trust that when the browser says a link is not secure, it is not secure.
- ☑ Use good password hygiene. Create strong passphrases (length trumps complexity) that are unique to each of your online accounts – never reuse the same password or passphrase for multiple accounts. Protect your passwords with a password manager such as Keeper, LastPass, Dashlane, or iCloud Keychain.
- ☑ Don't click on links or attachments in emails from an unknown sender, a suspicious sender or in emails that don't make sense. Attackers can "spoof" someone's email address to appear to be from anyone they choose. Never provide personal information to anyone in response to an unsolicited request. Never reply to unsolicited emails from unknown senders or open their attachments.
- ☑ Utilize Two Factor Authentication. This requires you to log into online accounts using something you know (password) plus something you have (fingerprint, face ID, PIN code from an app). You can set this up in the security/settings section of most online accounts.