BAIRD

Private Wealth Management

Your Checklist for Handling a Data Breach

It's an unfortunate circumstance that has happened to many: receiving an alert that your personal information may have been compromised as a result of a data breach. Even if it's unclear how much of your information has been leaked, you can still take steps to protect yourself as you move forward:

STAY UPDATED WITH ALERTS FROM THE COMPROMISED ORGANIZATION

When a breach occurs, an organization is legally required to make its consumers aware of it. Following that initial message, they may continue to post ongoing updates and disclosures about which customers were affected and how. Stay on the lookout for their most current information to help decipher exactly what of yours was stolen, like your:

- Username and password
- Payment information
- Social Security number
- Other identifying information, like a passport or driver's license number

CHANGE AND PROTECT YOUR PASSWORDS

After a data breach, one of your first tasks should be evaluating your most data-sensitive online accounts and changing those passwords. Consider accounts such as:

- Investment accounts
- Bank accounts
- Medical domains
- Email accounts
- Social media accounts

As you change your passwords, consider taking these extra measures as well:

- ☐ Avoid using duplicate passwords. A different password for every account is crucial – you don't want to give a hacker a skeleton key to your life.
- ☐ When possible, sign up for two-factor authentication. This way, any log-in attempt to your account outside of a trusted device must be approved through an app or text message on your phone.
- ☐ Use a trusted password manager. If you do so, logging into an account will only require you to remember the password you created for the password manager.

ALERT YOUR FINANCIAL INSTITUTIONS

In a data leak situation, it's hard to know exactly what of your information was taken. While organizations will issue disclosures about what they know has been compromised, data leaks can initiate a domino effect that results in other information being compromised outside of the breach. Because of this, it can be beneficial to alert your financial institution as a proactive safety measure.

- ☐ Cancel and replace your debit and credit cards. While you may not know whether your debit and credit cards have been compromised, it's better to be safe than sorry.
- ☐ Establish a trusted contact. By authorizing your Baird Financial Advisor to connect with a trusted family member or friend in situations of potential fraud, you add an extra layer of safety to your Baird accounts.
- ☐ If you suspect you have been fully compromised, place a fraud alert on your credit. Different from freezing your credit, this ensures any recent or new requests get additional scrutiny.

MONITOR YOUR ACCOUNTS AND CREDIT REPORTS

Look over your bank statements and credit card account activity from today through the date of the breach.

- ☐ Report anything on your bank statement or credit report that you find suspicious or don't remember.
- ☐ After reviewing any past activity, continue to keep a close eye on your accounts. This includes both the accounts from the organization that was breached and your financial accounts.

FREEZE YOUR CREDIT

The only surefire way to safeguard your credit after a breach is by freezing it. While this may feel like a hassle, it significantly hampers any identity thieves from using your credit information. And if you have two-factor authentication enabled, would-be thieves need your name, username, password, email, phone number and your physical phone to access your credit.

- ☐ Create an account with each of the three main credit bureaus (Experian, Transunion, Equifax) and place a freeze on your credit for free.
- ☐ Contact the agencies when you want to do anything that requires access to your credit score, like opening a new credit card or buying a car. This will put a temporary "thaw" on your credit.
- ☐ Refreeze your credit once you've accomplished the task you wanted.

DELETE YOUR DATA

You leave digital fingerprints and traces of information everywhere online, which data brokers collect and sell to advertisers, scammers and identity thieves. Fortunately, there are steps you can take to get your data out of the wrong hands.

- ☐ Contact data brokers to request all information they've collected on you be deleted – they are legally required to comply.
- ☐ Consider using a data cleanup service. If the task of contacting dozens (and potentially hundreds) of data brokers feels daunting, using a third-party service could be beneficial. These organizations will contact brokers on your behalf at a reasonable cost, and can remove almost all your personal data from the ether while guiding you on how to remove the rest.

REMAIN CAUTIOUS AND CONTINUE TAKING PREVENTATIVE STEPS

After you've experienced a data breach, it's in your best interest to continue taking protective measures. While you can't fully prevent future data breaches, you can set yourself up well to handle (what could be) the next one.

- ☐ Watch for spear phishing attempts, where bad actors use your hacked information to personalize their own hacking attempts. You can help protect yourself from these scams by:
    - Exercising caution with incoming calls and emails and verifying any communication before providing sensitive information.

Your Checklist for Handling a Data Breach *continued*

- Searching the inquiring organization's contact information and calling them directly to ensure the person on the other line is who they say they are.

☐ Consider using identity theft protection services that can monitor credit files, alerting you of any suspicious activity and helping you recover lost money and repair your credit score if you become an identity theft victim.

☐ Consider signing up for the credit monitoring services provided by the breached organization, but research alternatives first.

- Remember that Baird offers clients a third-party service that provides identity theft protection and helps you delete your online personal data.

Of course, if you're still feeling unsettled after a data breach, reach out to your Baird Financial Advisor – they will be happy to introduce you to identity monitoring services and provide other resources that may be helpful to you during this time.