Devising a Data Breach Game Plan

Presented by DiMatteo Group Financial Services Inc.

As you've likely read in the headlines, many companies have been victims of data breaches in recent years. For many of us, this situation can feel overwhelming. If businesses can't protect themselves from cyberattacks, what chance does the average consumer have?

Time to plan

The bad news is that we likely can't stop these data breaches from happening. But the good news is that, depending on the breach, it usually takes only a couple of key actions to reduce how you'll be affected—if at all. The secret lies in pinpointing the specific information that's at risk. Ask yourself, if attackers were to get ahold of *this* account, what could they access? From there, you can devise a simple game plan for almost any breach.

Credit and debit cards. A good place to start is by making safe choices when it comes to using your credit and debit cards. For example, enter payment information online only at HTTPS sites (as opposed to HTTP sites), never store your payment information on sites, and do business only with companies you trust.

Even when you make the right choices, however, your payment information will inevitably get out there. If you do catch wind of any breach of credit or debit card information, it's best to take the following steps:

- Review your recent card activity to see if any unauthorized charges have occurred.
- Report any unauthorized charges to your bank or credit card company.
- Request a replacement card.

Here, it's important to keep in mind that not all data breaches are properly disclosed. In fact, many aren't revealed until months (or even years!) after the compromise took place. Get in the habit of regularly monitoring your financial activity, and report anything suspicious as soon as you can.

Passwords. In the past few years, LinkedIn, Yahoo, and Twitter passwords have been exposed on a mass scale. What steps should you take when something like this happens again? First, change your password. But also ask yourself, *Have I used this password or a similar password for other online accounts?*

If you use a password in multiple places and just one of those places is breached, someone could access all accounts that use that password. The solution? Break the "password reuse" habit! That way, the next time an incident happens, you would have to change only the password to the site that was breached. To simplify this process, you might also consider adopting a password manager.

Enabling multifactor authentication can also help protect your account with an additional layer of security. For example, you might receive a smartphone or e-mail notification every time you use your password. So, if your password were ever exposed, an attacker would need that other form of authentication to log in—which he or she is unlikely to have.

Social security number. Unlike a password, you can't simply change a social security number when it has been exposed. What you can do is freeze your credit. As of September 2018, freezes are free, and they're the most heavy-duty tool at your disposal for protecting your credit. It's a preventive measure against (1) new lines of credit being opened in your name and (2) hard inquiries.

Some other tools worth looking into for an exposed social security number include:

- **Fraud alerts:** These alerts encourage companies to verify with you before opening new lines of credit.
- **Credit monitoring:** These tools monitor your credit in real time for any changes. They are *reactive* and not *proactive*; they alert you *after* the unauthorized activity happens.
- **Identity theft protection services:** For a hands-off approach to identity protection, these products offer tools and resources for one subscription fee.

Are you ready?
Now, let's apply what we've learned so far to a breach that doesn't fit so neatly into the categories above. In 2018, Facebook discovered a weakness that allowed attackers to take over any account. Attackers could find and reuse anyone's unique access token, allowing them to authenticate users' accounts. There was no known evidence of misuse, only the potential for it. Affected accounts were notified by Facebook via e-mail. If you received such a message today, what would you do?

You might start by asking yourself what your Facebook account has access to. With social media specifically, the answer depends on how you use your account.

- Does your profile have your real birth date?
- What third-party applications do you have connected to your Facebook account?
- Do you use Facebook Connect to log in to other online accounts—ones that might store your payment information?
- Have you ever messaged a family member your Netflix password, credit card information, or even social security number?

Once you identify what's at stake, identify the steps you can take to lock it down. Can you separate those connected apps—or at least change their passwords? Do you need to limit the type of information you post on Facebook? Can you monitor anything else that may have been exposed, like a credit card number?

Don't panic, do take action
Every breach is different. As such, there is no list of the "top three ways" to reduce impact across the board. But with a plan in place, there will be no need to panic when news of another breach hits the headlines. There will be the need to take action—and your data breach plan can help get you started. If a breach does affect you personally—to the point where someone is abusing your information and you can't figure out what to do next—we recommend checking out the helpful resources at IdentityTheft.gov.

DiMatteo Group Financial Services Inc.
1000 Bridgeport Avenue,Suite 506 | Shelton, CT 06484
203.924.5420 | 203.402.8305 fax