BALLENTINE PARTNERS

Risk Management

A Breach Has Occurred...Now What?

BALLENTINE PARTNERS | SAM GOUGH, CPF® | AUGUST 2015

With cyber theft often in the headlines, it might seem as though it's not a question of whether your personal information will be compromised, but when. For example, you have likely seen CNN's estimates that over 100 million Americans have had their personal information stolen and exposed over a one year period. This may leave you wondering, "How safe is my money?" While the question seems straightforward, the answer is complicated and depends on a number of factors: How did the breach take place? What information was compromised? How quickly was the issue identified and resolved? This paper details several scenarios that show you how best to mitigate your risk, regardless of the circumstance.

If my account numbers and/or login credentials are stolen and this leads to theft of assets, will I get my money back?

In most cases, where the breach occurred impacts how the bank or broker will respond. An institution is much more likely to restore your funds if their own system was compromised, rather than if your email or personal computer was infiltrated. If you gave your login credentials to someone and they used the information to initiate unauthorized withdrawals, the bank or broker will most likely hold you responsible for any transactions made by that person.

How do I get my funds restored if my information is stolen directly from my bank or broker and my money is stolen?

Generally, your bank or broker will reimburse your account if unauthorized withdrawals took place through no fault of your own and you notify the bank in a timely manner (typically within 60 days of the loss). Keep in mind that FDIC Insurance does not protect you from ID theft, unauthorized access to funds, or security breaches, as it was designed to prevent financial panics triggered by many depositors withdrawing cash and/or securities simultaneously. FDIC and SIPC will reimburse you if a bank or broker fails to have sufficient assets on hand to meet withdrawal requests, but they will not compensate victims in the event of loss due to fraud.

How does my risk of loss differ using a credit card versus a debit card?

If your credit card is stolen, under the Fair Credit Billing Act, you will not be held responsible for more than $50 of unauthorized charges. If your debit card number is stolen, and you still have your card, you are not liable for unauthorized transactions if you report them within 60 days of your statement date.

However, if your physical debit card is stolen, the amount you may be held responsible for depends on how quickly you report the loss to the card issuer:

If you report:	Your maximum loss:
Before any unauthorized charges are made	$0
Within 2 business days after you learn about the loss or theft	$50
More than 2 business days after you learn about the loss or theft, but less than 60 calendar days after your statement is sent to you	$100
More than 60 calendar days after your statement is sent to you	All the money taken from your ATM/debit card account, and possibly more; for example, money in accounts linked to your debit account.

Source: Federal Trade Commission Consumer Information

Should I be concerned if there is a security breach at a retailer where I have shopped?

Staying informed and aware is the key when it comes to retailer theft. If a retailer announces a breach and you may have been impacted given when you shopped there or the purchases you made, it is important to continue to stay vigilant and watch your accounts. Criminals can do a variety of things with stolen personal information: credit card information can be used to make online purchases or create counterfeit cards; other personal information such as your email address or account numbers can be used to send you a fraudulent email that attempts to entice you to click on a link that downloads malicious code onto your computer. The best way to mitigate these risks is to 1) sign up for a credit monitoring service like Identity Guard which will allow you to be notified in the event a criminal uses your information to open a fraudulent account (retailer security breaches often result in the retailer offering victims 1 year of this type of service free), and 2) be cautious before clicking on links in e-mails, even from "friends," as criminals can easily mask their sending address. We recommend clients retype URLs into their web address field rather than clicking through links.

How can I prevent a breach from happening in the first place?

Your primary focus should be on the security of your own digital devices, as it is more difficult to be reimbursed from the bank or broker for losses caused by a breach on your computer or cell phone. If you take measures to protect your personal devices and online accounts, the chances of a theft occurring significantly decrease.

There are several best practices you can adopt to mitigate your risks:

- Safeguard your personal computer systems:
- Secure any wireless networks at home with strong password protection, the latest and most aggressive security system (e.g. WPA2), and network/server names that are generic.
- Use anti-virus/anti-malware software products from a large, well-known company (e.g., McAfee, Symantec, Microsoft).
- Keep all software intertwined with the internet up to date, including your operating system, internet browser, and third-party plug-ins.

- Do not operate with admin-level privileges. Set up a separate profile on your operating system with only user-level privileges and use that profile for day-to-day email and web browsing. Use safe and strong passwords:
- Make your passwords alpha-numerical: Use at least 10 characters, including numbers, upper-case letters, lower-case letters, and special characters.
- Avoid using full words. This is particularly important if there is no authentication protection (e.g., locking a user account after 10 unsuccessful tries).
- Use multi-factor authentication whenever possible, especially with email accounts.
- Try not to use password reset security questions; if required, make them difficult.
- Use a different password for every online service.
- Consider using Dashlane or another password manager software to save complex passwords.
- Change passwords every six months or sooner if notified of a breach.

Summary

Generally, if your bank, broker, or retailer is compromised, you need not worry about a permanent loss of your funds, as long as you're vigilant and report any unauthorized transactions quickly. Your best defense is to set up strong systems for yourself and monitor all of your accounts on a regular basis. In all cases, staying informed and involved with all of your accounts is the key to preventing a loss.

About Sam Gough, CFP®

Sam is a Wealth Planner and his area of expertise is implementing clients' complex estate planning and investment strategies. Sam serves as a specialized resource for his clients, whose families often have extensive financial infrastructure including multiple family investment and charitable entities. In addition, Sam runs our Risk Management Knowledge Management team, which focuses on the advice and ideas we deliver to clients about how to manage and mitigate risks across their financial lives.

This report is the confidential work product of Ballentine Partners. Unauthorized distribution of this material is strictly prohibited.

The information in this report is deemed to be reliable but has not been independently verified. Some of the conclusions in this report are intended to be generalizations. The specific circumstances of an individual's situation may require advice that is different from that reflected in this report. Furthermore, the advice reflected in this report is based on our opinion, and our opinion may change as new information becomes available.

Nothing in this presentation should be construed as an offer to sell or a solicitation of an offer to buy any securities. You should read the prospectus or offering memo before making any investment. You are solely responsible for any decision to invest in a private offering.

The investment recommendations contained in this document may not prove to be profitable, and the actual performance of any investment may not be as favorable as the expectations that are expressed in this document. There is no guarantee that the past performance of any investment will continue in the future.

BALLENTINE
PARTNERS

info@ballentinepartners.com
https://ballentinepartners.com