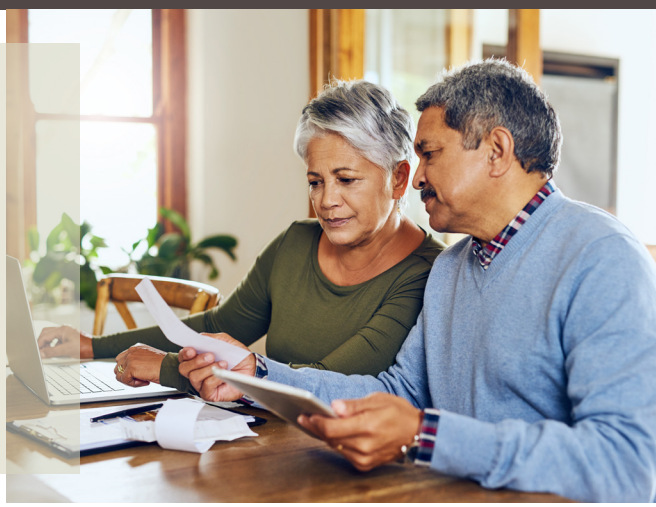
How to Protect Your Credit After a Data Breach



In 2024, we witnessed numerous significant cyber and ransomware attacks, as well as data breaches, impacting millions of people worldwide. Some of the most notable incidents involved major entities such as the cloud-data platform Snowflake, UnitedHealth Group, and Fidelity Investments. These cybersecurity breaches resulted in the theft of millions of customer records, including sensitive information like bank account details, credit card numbers, Social Security numbers, health insurance information, and medical records.

To illustrate the personal impact of such breaches, we introduce Mary, a fictitious character whose personal information was compromised during a security breach at a company she patronizes. With her data exposed, Mary is deeply concerned about the potential risks to her family's financial stability. Below, we outline the steps Mary is taking to safeguard herself and her family.

About Mary

Mary, a 61-year-old married woman, is planning to retire within the next two years. As a member of the sandwich generation, she cares for both her 85-year-old mother and her special needs son, Steven. Mary has accumulated several assets, including an investment portfolio, a Roth IRA with a balance of $2.8 million, and a special needs trust (SNT) for Steven, who has Down syndrome. At this stage in her life, Mary's primary focus is on financial conservation, making it crucial for her to take the necessary steps to protect her finances and preserve her legacy plans.

STEP 1: MARY DETERMINES WHAT INFORMATION WAS COMPROMISED

SCENARIO: Mary received an email from a popular online greeting card company that she has purchased from in the past that says her account has been involved in a data breach. The compromised information includes her:

- Full name
- Email address
- Password
- Data of birth
- Mailing address
- Bank account information

Before changing her password, Mary verified the legitimacy of the email by checking her credit monitoring software for any breach alerts and reviewing the company's recent press releases on their official website. She is aware that cybercriminals often send fraudulent emails claiming that information has been compromised, attempting to lure individuals into logging into spoofed websites to steal their data.

STEP 2: MARY SECURES HER ACCOUNTS

SCENARIO: After verifying the breach, Mary took immediate action to secure her accounts by changing her passwords and PINs. She realized that she had used the compromised password on another online account as well. To enhance her security, she utilized her internet browser's complimentary password manager to generate a new, strong password composed of randomized numbers, letters, and characters, making it difficult for hackers to crack.

While researching additional steps to take after her account was compromised, Mary discovered two-factor authentication. Enrolling in two-factor authentication is one of the simplest and most effective ways to add an extra layer of protection to your accounts. With two-factor authentication, Mary receives a push notification on her phone or a time-sensitive code via email to confirm her identity each time she logs in, making it significantly harder for hackers to gain access to her accounts.

STEP 3: MARY ACTIVELY MONITORS AND LOCKS DOWN HER CREDIT FILE

SCENARIO: Following the data incident, Mary became increasingly worried about someone using her leaked information to open accounts in her name. To monitor her credit activity, she created accounts with each of the major credit bureaus: Experian, TransUnion, and Equifax. Through these websites, Mary can check if someone has stolen her identity or used her bank account information by reviewing her active lines of credit. Given the ongoing nature of data threats, it is recommended that she checks her credit report every three months.

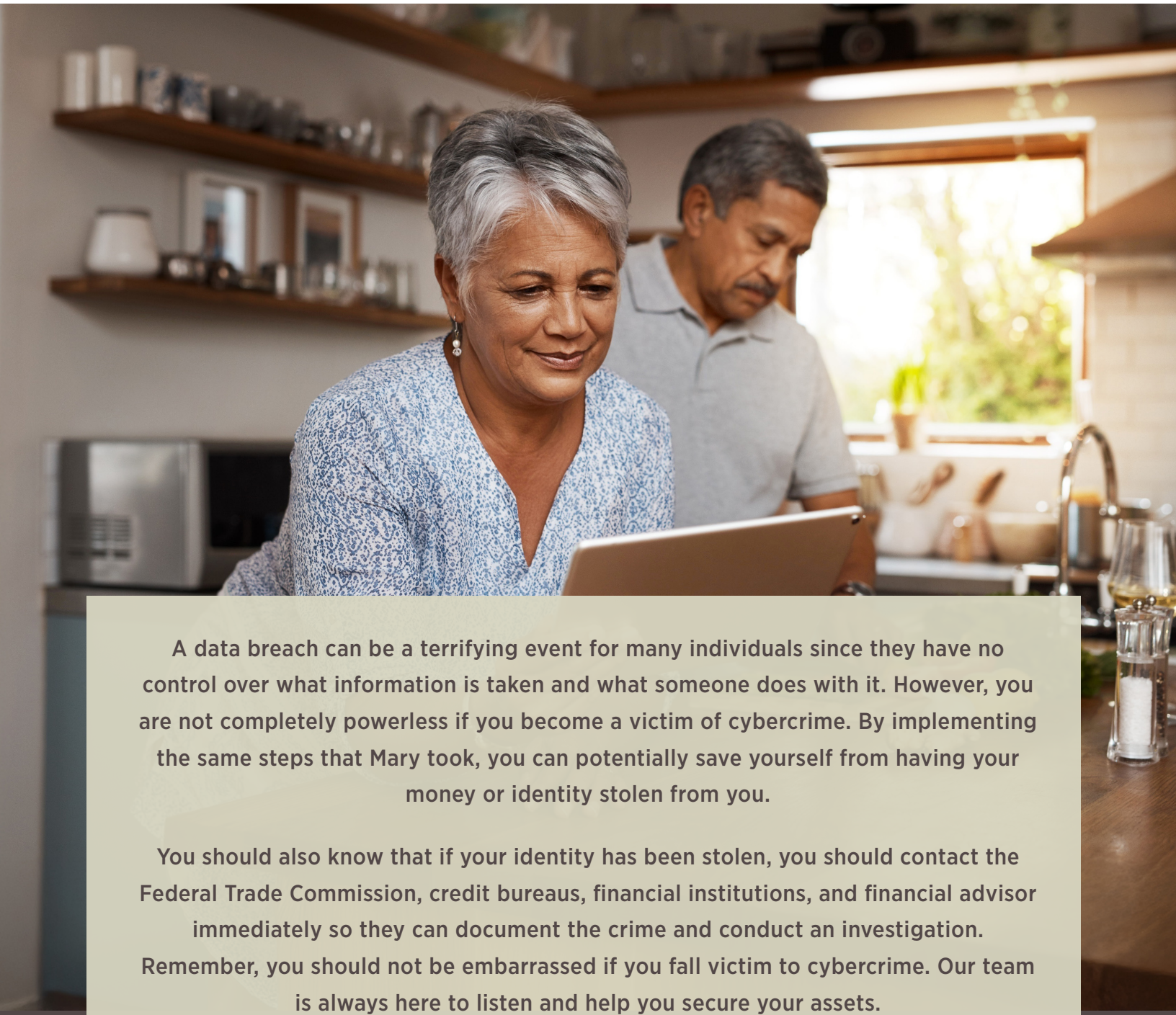
Mary also decided to verify if any money had been withdrawn from her retirement account and her son's special needs trust. As a high-net-worth individual, she is an attractive target for scammers seeking access to her assets. By reviewing her printed records, she can confirm that the balances in each account are accurate.

Additionally, Mary can take further steps to protect her finances by locking her credit and Social Security number. Credit freezing is a strategy that prevents anyone, including herself, from applying for credit in her name unless she contacts the credit bureau to unlock it. This also blocks lenders and other companies from accessing her credit files.

Similarly, Mary can lock her Social Security number to prevent it from being electronically accessed or used for job applications by contacting the Social Security Administration (SSA). The lock must be administered by the SSA, so she would need to call their office at 1-800-772-1213. However, she can self-lock her number from being used for employment purposes by creating an E-Verify account online. Since Mary does not plan to take out a new line of credit or start a new job within the next year, locking both her credit and Social Security number is a sensible precaution for her situation.

STEP 4: MARY CHECKS FOR ANY SUSPICIOUS BEHAVIOR ON HER DEVICES

SCENARIO: Knowing that her personal information is out on the dark web, Mary has become vigilant about unusual activity within her online accounts and device. Since the breach, she's received multiple emails from her email provider stating that someone is trying to log into her email account. Luckily, the hacker is unable to get in because she has strengthened the integrity of her password and has added a two-step verification to the account.



A data breach can be a terrifying event for many individuals since they have no control over what information is taken and what someone does with it. However, you are not completely powerless if you become a victim of cybercrime. By implementing the same steps that Mary took, you can potentially save yourself from having your money or identity stolen from you.

You should also know that if your identity has been stolen, you should contact the Federal Trade Commission, credit bureaus, financial institutions, and financial advisor immediately so they can document the crime and conduct an investigation. Remember, you should not be embarrassed if you fall victim to cybercrime. Our team is always here to listen and help you secure your assets.

E / contact@6meridian.com • *P* / 316.77.4601 / 855.334.2110 • *F* / 316.776.4260

WWW.6MERIDIAN.COM • 8301 E 21st St N, #150, Wichita, KS 67206

DISCLOSURES

6 Meridian is a group comprised of investment professionals registered with Hightower Advisors, LLC, an SEC registered investment adviser. Registration as an investment advisor does not imply a certain level of skill or training. Some investment professionals may also be registered with Hightower Securities, LLC, member FINRA and SIPC. Advisory services are offered through Hightower Advisors, LLC. Securities are offered through Hightower Securities, LLC. All information referenced herein is from sources believed to be reliable. 6 Meridian and Hightower Advisors, LLC have not independently verified the accuracy or completeness of the information contained in this document. 6 Meridian and Hightower Advisors, LLC or any of its affiliates make no representations or warranties, express or implied, as to the accuracy or completeness of the information or for statements or errors or omissions, or results obtained from the use of this information.

6 Meridian and Hightower Advisors, LLC or any of its affiliates assume no liability for any action made or taken in reliance on or relating in any way to the information. This document and the materials contained herein were created for informational purposes only; the opinions expressed are solely those of the author(s), and do not represent those of Hightower Advisors, LLC or any of its affiliates. 6 Meridian and Hightower Advisors, LLC or any of its affiliates do not provide tax or legal advice. This material was not intended or written to be used or presented to any entity as tax or legal advice. Clients are urged to consult their tax and/or legal advisor for related questions

Third-party links and references are provided solely to share social, cultural and educational information. Any reference in this post to any person, or organization, or activities, products, or services related to such person or organization, or any linkages from this post to the web site of another party, do not constitute or imply the endorsement, recommendation, or favoring of 6 Meridian or Hightower Advisors, LLC, or any of its affiliates, employees or contractors acting on their behalf. Hightower Advisors, LLC, do not guarantee the accuracy or safety of any linked site