NFP
An Aon Company

Property & Casualty
Personal Risk

Identity Theft: 7 Steps to Take After a Data Breach

Mila Araujo, Personal Cyber Practice Leader, AVP, Digital Shield, Property and Casualty

Data breaches like the recent National Public Data breach which exposed sensitive data including Social Security numbers, are becoming more common and severe. Today, data breaches are impacting millions of individuals and businesses each year.

While a data breach might not result in immediate financial loss for some, it can lead to various forms of cybercrime not limited to identity theft, such as AI enabled fraud, online fraud, pig butchering, cyberbullying, sextortion and social engineering.

That's why it's crucial to take a proactive approach in protecting your information.

Being the victim of a data breach can be overwhelming, but taking the right steps can help secure your information and reduce the impact.

Some forms of identity theft are:

- General Identity Theft: Unauthorized use of your information to open new accounts or make purchases.
- Medical Identity Theft: Using your identity for medical services or prescriptions.
- Tax Identity Theft: Filing fraudulent tax returns to claim refunds in your name.
- Financial Identity Theft: Opening bank accounts or taking out loans under your name.
- Criminal Identity Theft: Using your identity for illegal activities, potentially creating false criminal records.
- Children's Identity Theft: Using a minor child's personal information, such as name and Social Security number, usually to obtain credit or employment.

What can you do if your personal information has been compromised? Here are seven steps you can take to mitigate the damage and regain control of your life.

1. Fraud Alerts and Credit Freezes

If you think your data has been compromised, your first move should be to place a fraud alert with one of the major credit bureaus. This automatically notifies the other two, and you'll receive confirmation by mail. If you're not planning to apply for new credit, consider freezing your credit. It's free and prevents unauthorized access to your credit report. Check out services like **Frozen Pii** to secure your Social Security and IRS accounts at no cost.

2. Get a Credit Report

After a breach, make sure to keep an eye on your credit. Take advantage of reputable credit report services. Some credit report services – such as **annualcreditreport.com** – also offer free services. Take the time to regularly review your credit and accounts for any unfamiliar accounts or suspicious activity.

3. Online Accounts

A data breach often means that your online accounts are at risk. Secure your security by using a password manager to create complex, unique passwords for each account. You can also consider using different email aliases for sensitive accounts to minimize exposure.

Lastly, enable multifactor authentication (MFA) wherever possible to add another layer of protection.

4. Protect Your Phone and Mobile Accounts

Heard of SIM swapping? **SIM swapping** is when criminals take over your phone number to access your accounts. Bad actors can hijack your phone and attempt to gain access to your financial and personal account by requesting verification codes be sent to your phone.

To avoid this, reach out to your mobile provider and set up a PIN or additional security options.

5. Be Alert and Mindful of Phishing

Be extra cautious of unsolicited calls or emails asking for personal information because they could be phishing attempts aimed at collecting even more data. Check email addresses carefully, and always verify with whom you are speaking to. When in doubt, call the person back at the number you normally would reach them at to avoid being tricked by deep fakes and other cyber criminal ploys.

6. Personal Cyber Insurance is Essential

Cyber insurance is more than just a safety net, it gives you access to cybersecurity experts and financial coverage for identity theft and online scams. Don't wait for a breach, consider adding a dedicated personal cyber policy to stay fully protected and gain access to 24/7 personalized assistance and resources by **learning more or signing up today**.

7. Report Identity Theft to the FTC

If you've confirmed that your identity has been stolen, report it to the Federal Trade Commission (FTC) at **identitytheft.gov**. This will help you establish a recovery plan and take the necessary steps to secure your information.

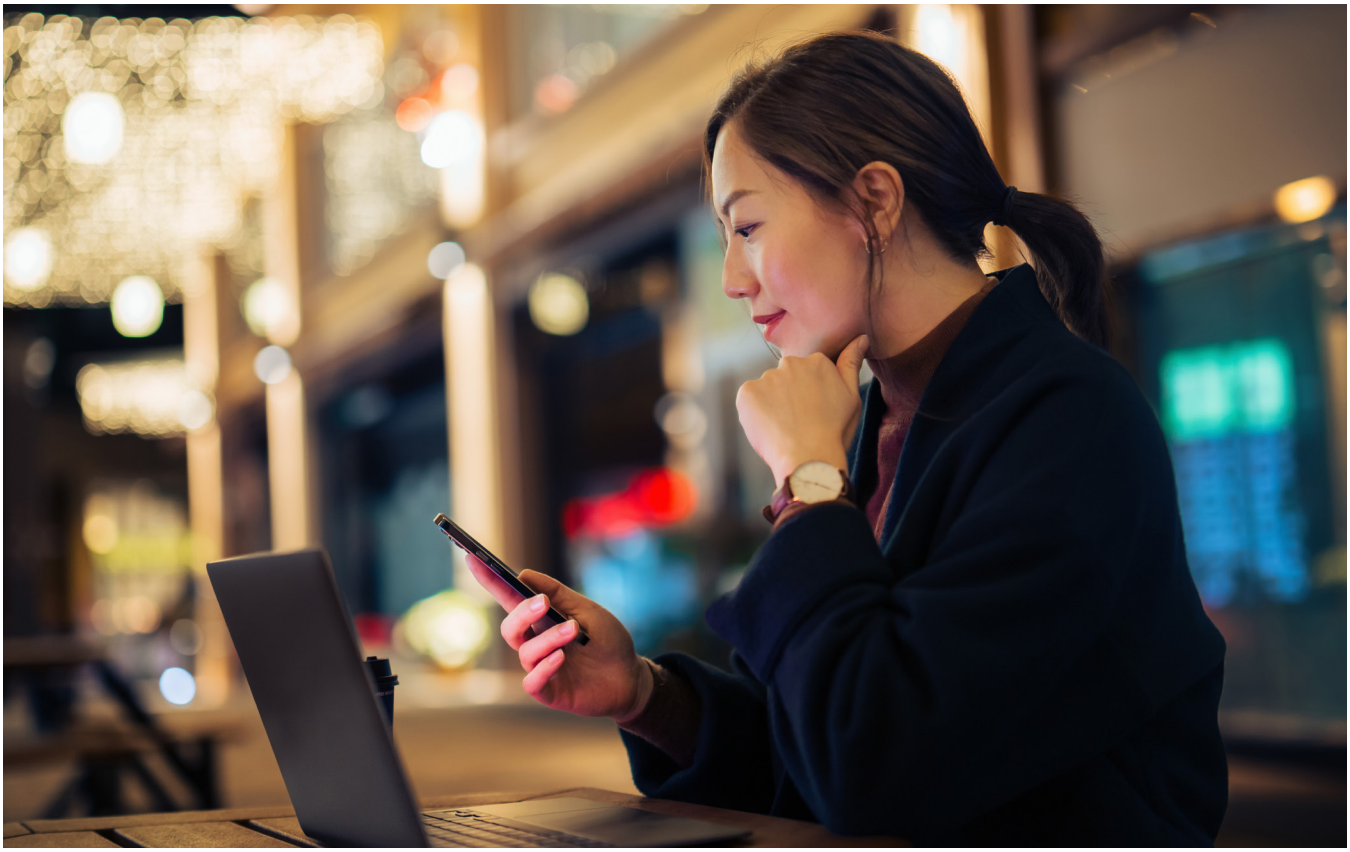
Why Choose NFP?

At NFP, we understand that each case is unique, and we have the resources to help keep you educated and secure.

Our partnerships with the leading personal cybersecurity insurers allow us to offer our clients top-tier tailored security solutions and expert guidance. From setting up MFA, ongoing support and comprehensive security assessments, we ensure that you are equipped to handle cybersecurity threats.

To learn more about safeguarding yourself and your family against cyber threats, sign up online or contact us today.

Learn More



Mila Araujo
Personal Cyber Practice Leader, Assistant Vice President, Digital Shield
Property and Casualty
P: 332.400.2627 | **mila.araujo@nfp.com**

For your business.
For your people.
For your life.

NFP.com

NFP
An Aon Company