19 Tips for Breach Victims in 2023

Proactively protecting your credit and identity data is critical to reducing your risk of fraud and loss.

CONTROL ACCESS

1 **Check Your Passwords on All Accounts** Change your exposed account credentials immediately, and then update any other accounts that use the same or similar password. Moving forward, use unique passwords or passphrases for every account to avoid credential stuffing.

2 **Enable Multi-factor Authentication (MFA)** More secure than a password, multi-factor authentication requires at least two inputs to verify who is accessing an account — such as your password and one-time code sent via text message. The extra step can keep identity thieves from accessing your accounts when they only have a compromised password.

3 **Freeze Your Credit Report** A credit freeze stops unauthorized viewing of and access to your credit report by new creditors and potential thieves. Credit freezes must be set (and removed) at each of the three bureaus.

4 **Secure Your Device** Make sure you have enabled the lock screen of your mobile device with a PIN or biometric passcode. Turn on the “Find My” device feature so you can disable the device or delete your information if it’s lost or stolen. You may want to consider installing a mobile identity monitoring solution that also detects malware, spyware and other exploitable weaknesses.

5 **Don’t Overshare** Cybercriminals use personal information posted on social media to impersonate you when creating or accessing accounts. Be mindful of how the information you share could be misused.

SET UP ALERTS

6 **Take Advantage of Credit Report Monitoring** Credit monitoring services can spot the opening of potentially fraudulent new accounts or even misuse of your existing accounts. Many include a feature which sends you updates when there are changes to your credit report. There are many monitoring options — some free and some paid — and you should select the type of monitoring with which you are the most comfortable.

7 **Place Fraud Alerts on Your Credit Report** A fraud alert advises those making an inquiry into your credit report to be more cautious (both for existing and new account activity) and that they should take additional steps to verify the applicant’s identity.

8 **Enable Activity Alerts for Your Accounts** Receiving mobile or other text alerts to detect possible fraudulent activity on your social media or online shopping accounts is even more important after a breach. Adjust these to strike the right balance of alert activity for your needs.

9 **Activate Alerts for Credit and Debit Card Accounts** Notifications for suspicious transactions (e.g., unusual login attempts, contact information change) can quickly detect suspicious activity on your credit or debit card. Many banks support text messages, email or in-app alerts.

10 **Set Alerts for or Lock Online Card Transactions** Typically, card data stolen in an online merchant breach can only be used for fraudulent purchases online as well. Setting up alerts for online transactions can help quickly detect suspicious activity without creating unnecessary alerts for purchases at physical stores. By locking your card and only unlocking it when you make purchases, you limit the opportunities for anyone else to use your account. Consider using one card for online purchases and another one for in-person shopping that is locked from online purchases.

STAY VIGILANT

11 **Scan Criminal Marketplaces** Whether it was compromised in a healthcare-, governmental- or finance-based data breach, knowing that your credit and identity information could be used to conduct fraud in your name is an important first step to making changes elsewhere that can minimize the impact. Free services, including Firefox Monitor and Have I Been Pwned?, can scan where personal data is available online.

12 **Monitor Your Social Media and Email** Imposter accounts and account takeovers can lead fraudsters to scraping personal information to target you or your connections with social engineering attacks, or to buy and sell that compromised data on the Dark Web. Set up notifications for unusual login attempts, changes to contact information or other suspicious activity.

13 **Beware of Social Engineering** When your contact information is exposed (e.g., phone number, email or street address), you may be contacted by criminals pretending to be a trusted authority to scam you into sending money or revealing additional private details to commit more targeted fraud.

14 **Guard Against Multi-Channel Scams** Complex, multi-stage scams use a combination of emails, phone calls and fraudulent websites to create a realistic experience for a victim designed to trick them into revealing personal or payment information.

15 **Order Free Copies of Your Credit Reports** Regularly review your credit reports to identify inaccuracies and spot potentially fraudulent activity. The three nationwide credit reporting agencies — TransUnion, Equifax and Experian — offer weekly access to your reports.

MAKE CONTACT

16 **See If You Need a Replacement Card** If they don’t replace it automatically, contact your financial institution to see if you need a replacement debit or credit card. Security features (e.g., alerts and card controls) may reduce your risk without the inconvenience of replacing the potentially compromised card.

27 **Activate USPS Informed Delivery** The Informed Delivery service allows you to digitally view mail and packages that are set to be delivered to your address, so you know when to expect important mail (like replacement cards), reducing the risk of mail theft. Find out more at the post office’s website.

18 **Notify the DMV of Your Stolen Driver’s License** Alert state agencies and law enforcement of the theft of your driver’s license number or physical license so they’re aware someone might impersonate. Better yet, ask the DMV if it will change your driver’s license number to protect you against impersonation.

19 **Contact the Social Security Administration** Request your wage earnings report to verify that your Social Security number is not being used fraudulently, which could result in your owing taxes for wages earned by someone using your stolen information.

These recommendations can help, but understand that not all are appropriate for every breach. Consulting with an identity restoration advisor or identity protection service can help ensure you take the steps needed to respond to the risk of your unique situation.

IdentityForce®
A TransUnion® Brand

ITRC IDENTITY THEFT RESOURCE CENTER

NOW FEATURED ON Family Security Today