21 Tips for Breach Victims in 2022

When your personally identifiable information (PII) has been compromised in a data breach, you can take steps to reduce further cyber fraud.

CHANGE YOUR ACCESS

1. **Change Your Passwords on Other 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. **Adopt 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 a one-time code sent via text message and your password. The extra step can prevent identity thieves from accessing your accounts when they only have a compromised password.
3. **Freeze Your Credit Report** A credit freeze prevents unauthorized viewing of and access to your credit report by new creditors, background check companies, and potential thieves. Credit freezes must be set (and removed) at each of the three bureaus. Credit freezes are free in all 50 states.
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.
5. **Don't Overshare** Cybercriminals use personal information posted on social media to impersonate you when creating or accessing accounts. Make sure you only share personal details with people you trust.

SET UP ALERTS

6. **Set Up Credit Report Monitoring** Credit monitoring services can spot the opening of potentially fraudulent new accounts or even misuse of your existing accounts. Many also have the advantage of sending you updates based on ongoing usage, rather than relying on you to check in with them or only allowing you to get an update once a year. 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 when using it (both for existing and new account activity), typically requiring them to take additional steps to verify the applicant's identity.
8. **Protect Your Mobile Device** Set up monitoring on your mobile devices to detect malware, spyware, and other exploitable weaknesses. Look for an identity theft protection service with mobile cybersecurity built into its app.
9. **Enable Multi-Account Activity Alerts** Receiving mobile or other text alerts to detect possible fraudulent activity is even more important after a breach. Adjust these to strike the right balance of alert activity for your needs.
10. **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.
11. **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.

BE ON THE LOOKOUT

12. **Scan Criminal Marketplaces** Identify where your personal data is already available. It could be combined with your breached information to conduct fraud in your name. Free services, including Firefox Monitor and Have I Been Pwned?, can scan where personal data is available online.
13. **Monitor Your Social Media Accounts** Imposter accounts and account takeovers through social media can lead to fraudsters scraping personal information, targeting you or your connections through social engineering, then buying and selling your personal information on the dark web.
14. **Beware of Social Engineering** When your contact information is exposed (e.g., phone number, email, or street address), you're likely to be contacted by criminals pretending to be a trusted authority to obtain even more private data to commit more targeted fraud.
15. **Monitor for Suspicious Email Account Activity** If your email provider supports alerts, set up notifications for unusual login attempts, changes to contact information, or other suspicious activity so you can quickly detect fraud.
16. **Review Your Records with the Medical Insurance Bureau (MIB)** Just like your credit reports, consumers are legally entitled to annual access to their records with the Medical Insurance Bureau (MIB). Your MIB consumer file can be requested digitally here: https://www.mib.com/request_your_record.html

MAKE CONTACT

17. **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 — are required to provide you with access to your reports once a year (and, now, each of the agencies is providing reports once per week).
18. **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 card. Security features (e.g., alerts and card controls) may reduce your risk without the inconvenience of replacing the potentially compromised card.
19. **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.
20. **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 to change your driver's license number to protect you against impersonation.
21. **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.

SONTIQ™ A TransUnion® Company

ITRC | IDENTITY THEFT RESOURCE CENTER

NOW FEATURED ON Family Security Today