2021 | 10 TIPS

FOR DATA BREACH VICTIMS

WHEN YOUR PERSONAL INFORMATION IS EXPOSED

1 Beware of Stolen Funds

Review your bank and financial accounts and immediately report any stolen funds to your financial institutions.

2 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.

3 Request a Free Copy of Your Annual Credit Report

Review your report and contact credit report company directly about any inaccurate information. An additional resource is the Identity Theft Resource Center, 888-400-5530. Subscribe to an identity/credit monitoring service for alerts, if your information is being compromised.

4 Confirmed Victim of Identity Theft? Create an Identity Theft Report with The Federal Trade Commission (FTC)

Expect law enforcement to request a copy of this report when you contact them. Learn more here: *www.identitytheft.gov*.

5 Place an Extended Fraud Alert or Security Freeze on Your Credit

Extended fraud alert allows creditors access to your file after they contact you to verify your identity before extending credit. A credit freeze prevents creditors from accessing your credit file completely. To request one, call each credit bureau directly. Laws vary by state.

6 Enable Two-Factor Authentication (2FA)

2FA helps protect your online accounts from unauthorized access. With 2FA, use something you know (your username and password) and something you have (a one-time code sent to your phone) to verify your identity and log in to your account.

7 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 who's stolen your information.

8 Contact Your Health Insurance Carrier

Request a copy of your health insurance statement in order to identify any fraudulent medical claims.

9 Audit Your Login Credentials

Change passwords for all online accounts and sign up for a password manager tool to store all your login credentials in one secure location.

10 Protect Your Mobile Device

Reduce risks of future identity incidents by monitoring your mobile devices for malware, spyware, and other exploitable weaknesses. Look for an identity theft protection service with mobile cybersecurity built into its app.

To activate your identity theft protection at no additional cost, visit https://cigna.identityforce.com/starthere or call 833-580-2523.

961163 10/21