Fraud Recovery & Identity Protection

Chartway CREDIT UNION

Immediate Actions:

- ☐ Contact your financial institutions IMMEDIATELY to report any fraudulent activity or unrecognized transactions. They will be able to block or close any compromised accounts/cards. You can also block your cards through online banking as soon as you notice anything suspicious.
- ☐ Change your username and password associated with your compromised accounts. We recommend using different usernames and passwords for each online platform. For security, usernames should NOT include parts of your name, birthdate, or email address.
- ☐ Utilize multi-factor authentication for online accounts if available.
- ☐ Review your credit report for unauthorized loans or inquiries. Request a free copy of your credit reports from all three credit bureaus: Equifax, Experian, and TransUnion.
    - ☐ (877) 322-8228 https://www.annualcreditreport.com
- ☐ If your social security number has been compromised, place a fraud alert/credit freeze on your credit report with all three credit bureaus to prevent fraudulent loan applications.
    - ☐ Experian: (888) 397-3742 https://www.experian.com
    - ☐ Equifax: (888) 378-4329 https://www.equifax.com
    - ☐ TransUnion: (888) 909-8872 https://www.transunion.com
- ☐ Review ChexSystems report to ensure unauthorized bank accounts have not been opened. If your social security number has been compromised, place a security freeze to prevent fraudulent account openings.
    - ☐ (800) 887-7652 https://www.chexsystems.com

Reporting Fraud:

- ☐ File a report with the Federal Trade Commission at https://www.reportfraud.ftc.gov
- ☐ File an identity theft report at https://www.identitytheft.gov
- ☐ File a report with the Internet Crime Complaint Center at https://www.ic3.gov
- ☐ File a report with your local police department. Obtain a copy of the report or the report number and detective's name.

Fraud Recovery & Identity Protection

Chartway CREDIT UNION

Secure Your Accounts:

- ☐ Place verbal passwords on all your accounts if available.
- ☐ Contact your cell phone carrier to ensure no unauthorized changes have been made to your phone plan, such as call forwarding or cloning. Add a verbal password on this account as well.
- ☐ Scan your devices for malware, spyware, viruses, and other potential threats.

Monitor Your Accounts:

- Frequently review your account statements and credit reports for unauthorized activity.
- Consider enrolling in a credit monitoring service to help detect and prevent fraudulent activity.

Reminders to Avoid Scams:

- Never click on links sent to you in an email or text message, unless you are certain they are legitimate.
- Never provide confidential information by phone, email, or text. For example: social security number, username, password, account/member number, debit/credit card numbers, secure access codes, etc.
- Fraudsters use scare tactics, such as threatening to disable your account. Don't feel pressured into providing any personal information or codes.
- Be cautious of fraudulent phone calls that claim to be from the Fraud Department. The phone number on the caller ID may appear to be coming from a legitimate source but it is really a fraudster masking the phone number to gain personal information from you. This tactic is called "spoofing" a phone number. Ask the caller for their name and a phone number that you can call them back at. If the phone number they tell you to call back does NOT match the caller ID, this is a major red flag. Hang up and call the business back from a trusted phone number to confirm if the call was legitimate.