How to Safeguard Your Fairmont Federal Credit Union Accounts and Protect Your Identity When You are Involved in a Third Party Data Breach.

Assess the Situation

While it can be very unnerving to receive notification that your personal information has been compromised in a security breach, please know that millions of people every year receive such notification but they do not become victims of identity theft. This isn't to say that you should take the situation lightly. The first thing to do gain as much information as you can about the data breach including what information was included in the compromise. If a police investigation is not underway, then you may notify the proper authority.

Notify the Service Providers

Notify the appropriate service providers depending upon the type of information that was stolen.

For financial account, debit card and credit card numbers, contact the financial service providers and/or card issuers to report the incident and to:

- Close all affected accounts and open new accounts with new numbers.
- Cancel all affected debit and credit cards; have them blocked as stolen.
- Request a passcode to protect your account.
- Monitor your accounts closely and reconcile monthly statements promptly.
- Report any fraudulent activity immediately.

For your Social Security Number, contact your financial service providers and the credit reporting agencies to:

- Put your financial service providers on notice and request a passcode to protect your account.
- Ask the credit bureau how a fraud alert works and request one be added to your record if you are comfortable with the stipulations it imposes. Do so with each of the credit reporting agencies.
- Request your free copy of the credit report. Explain that your SSN was compromised in a data breach and that you are a potential victim of identification theft. Contact numbers for the credit bureaus are listed below.
- Check your credit reports closely for irregularities and report them to the applicable bureau.
- Review your credit reports quarterly for at least one year and at least semi-annually thereafter.
- Consider using a credit report monitoring service. There is usually a cost to this service, but it may be worth the price if it aids in quickly detecting ID fraud or account takeovers.
- Request credit reports on your children if their SSNs could have been compromised as it is not uncommon for criminals to use children's identities to establish fraudulent credit.

For other types of personal data compromises, the following actions may be taken:

- If your insurance policy information is involved, contact your insurance agent and request the company change your policy/account number.
- If Human Resource data was compromised, request policy/account number changes for your 401K, life insurance, and stock option holding accounts. Also request passcode protection for such accounts or change existing codes.
- If your driver's license is stolen, contact your state Department of Motor Vehicles and notify them of the theft, but don't Expect a change in your license number.

Safeguard Your FFCU Accounts

Visit your nearest full-service Fairmont FCU office and provide one of our Financial Service Representative (FSR) with details of the data breach so the FSR can perform a risk assessment.

Bring with you a valid photo ID and a document that shows your name and address such as a voter's registration card, a utility or credit card bill, proof of insurance or a property tax invoice or receipt.

Permit our FSR to capture your photo and signature so we can ensure we are serving you and only you when you visit our offices.

Close all of your accounts that may have been compromised including debit and credit cards.

Open new Fairmont Federal Credit Union accounts and cards. The credit union will provide new checks and cards free of charge.

Provide the FSR with an additional account passcode to be used when you conduct CU business by phone with a CU employee.

Change all other user and log-on IDs, passwords, or PINs that have been compromised. For instance, if your social security number was included in the data breach and you use the last four digits of your SSN as your Telephone Banking PIN, then you should change the PIN immediately.

Other ID Protection Tips

- Only give your Social Security Number when it is absolutely necessary. Ask if another type of ID can be used instead, such as a driver's license number.
- Never put your Social Security Number on checks and don't carry your SSN card in your wallet.
- Before revealing any personal financial information, verify whom you are dealing with, how it will be used, and if it will be shared with others.
- Keep items and documents with personal information in a safe place and either shred or tear them up when you don't need them any longer.
- Make a photocopy (front and back) of all identification, financial, and insurance cards that you carry in your wallet and keep it in a safe place. If your wallet is lost of stolen, you'll have all the information you need to promptly and accurately report the loss.
- When you sign the back of your financial cards also include "Check Photo ID".

Item of Less Concern

Information that is readily attainable from public sources such as names, addresses, phone numbers, and birth dates do not pose a serious threat to identity theft as thieves cannot do much with that information alone. If however, this information is lost, stolen, or compromised in conjunction with the various types of financial data described previously then action should be taken.

Credit Bureau Contact Information

- Experian - 888.397.3742 or www.experian.com
- Equifax - 800.685.1111 or www.equifax.com
- Trans Union - 800.916.8800 or www.transunion.com

Other Resources

If you do become a victim of identity theft you may contact the following agencies to obtain information on dealing with and recovering from ID Theft:

- Federal Trade Commission at 877.438.4338 or www.consumer.gov/idtheft
- Identity Theft Resource Center at www.idtheftcenter.org

The information contained in this document is meant only to provide consumer tips to our credit union members regarding data breaches and protecting their personal data. It should not be relied upon as the sole source of information on preventing, deterring, detecting, or combating identity theft.