TIPS TO PROTECT YOUR IDENTITY

MONITOR YOUR ACCOUNTS REGULARLY

- ✓ Keep a close eye on your credit union accounts and any other financial accounts you may have. Look for any unfamiliar transactions or changes. If you notice anything suspicious, report it to us or your financial account provider immediately.
- ✓ Add a codeword to your account. This will be requested when your account is accessed in a branch, by phone, or electronic communication.
- ✓ Set up account activity notification alerts. This feature can be activated in online banking. For other financial accounts, contact your provider to explore options.

UPDATE YOUR PASSWORDS

- ✓ Change your passwords, especially for any accounts associated with the email address or phone number potentially exposed. Use complex passwords that combine letters, numbers, and symbols, and avoid reusing passwords across different accounts.

AVOID CHECK WASHING

- ✓ When writing checks, use black gel pens. The ink found in blue ballpoint pens can be easily removed. When writing a check, do not leave gaps or large spaces between words and numbers.
- ✓ Instead of placing bill payments in your mailbox, take the mail directly to your carrier or drop it off inside the post office. Avoid using the blue outdoor postal mailboxes, as they are more vulnerable to tampering. Retrieve mail daily and never leave the mailbox full overnight.

BE WARY OF PHISHING ATTEMPTS

- ✓ Be cautious of emails, texts, or calls that ask for personal information or prompt you to click on links. Fraudsters often use this information to trick you into giving away your credentials. Always verify the sender's identity before responding.
- ✓ Your financial institution or company you do business with will never ask for your online banking username or password, account reset codes, PIN, debit/credit card numbers, social security number, account information, or ask you to send funds or purchase gift cards.

ENABLE TEXT VERIFICATION CODES

- ✓ Wherever possible, enable text verification codes on your accounts. This extra layer of security requires you to verify your identity through a second method, such as a text message or an authentication app, making it harder for unauthorized users to access your accounts. It increases the security of your account.
- ✓ As an increased security measure, you may be asked to receive and confirm a text verification code sent to your phone. This helps protect access to your account when in a branch, on the phone or communicating with us electronically.

REPORT SUSPICIOUS ACTIVITY

- ✓ If you believe your identity has been compromised, report it immediately to the Federal Trade Commission (FTC) at IdentityTheft.gov. Also, contact your financial institutions to notify them of the potential fraud.

CHECK FRAUD PREVENTION

- ✓ Consider using online and mobile banking services to transfer funds or person-to-person payments.
- ✓ Shred or burn canceled checks, mobile-deposited checks, credit card statements, and bills after 30 days, and keep your checkbooks stored securely at home.
- ✓ Making checks payable to specific individuals or businesses enhances security, so it's best to avoid writing checks payable to "cash."

CHECK YOUR CREDIT REPORTS

- ✓ Regularly review your credit reports for any new accounts or inquiries you do not recognize. You can obtain free credit reports annually from each of the three major credit bureaus at AnnualCreditReport.com.

Enrichment federal credit union

Enriching lives. Empowering futures.

PLACE A FRAUD ALERT OR FREEZE CREDIT REPORTS

Fraud Alert: A fraud alert is a warning placed on your credit report that tells creditors to take extra steps to verify your identity before issuing credit in your name. This can be particularly helpful if you believe your personal information may have been compromised, this makes it harder for identity thieves to open new accounts. A fraud alert will not affect your existing accounts or prevent you from using your credit cards.

How to Place a Fraud Alert:

- You can request a fraud alert by contacting any one of the three major credit bureaus listed below (Equifax, Experian, TransUnion). Once you place the alert with one bureau, they are required to notify the other two, so your alert is added to all three of your credit reports.

Equifax	Experian	Transunion
www.Equifax.com	www.Experian.com	www.Transunion.com
800-685-1111	888-397-3742	800-916-8800

- The initial fraud alert remains in place for one year and can be renewed after it expires. You can also request an extended fraud alert, which lasts for seven years. A police report or other documentation showing you are a victim of identity theft is required for this type of alert.

Credit Freeze: A credit freeze (also known as a security freeze) is a more robust protection that locks your credit report, it restricts creditors or identity thieves from accessing your report entirely. This means that new credit accounts cannot be opened in your name while the freeze is in place. Unlike a fraud alert, a credit freeze does not expire and remains in place until you remove it or grant someone access.

How to Place a Credit Freeze:

- To place a credit freeze, you must contact each of the three major credit bureaus individually.
  Here's how:
  - Equifax: Visit the Equifax website or call their automated line to request a freeze.
  - Experian: You can place a freeze online through the Experian website or by phone.
  - TransUnion: TransUnion also allows you to freeze your credit via their website or by calling their support number.

Equifax	Experian	Transunion
www.Equifax.com	www.Experian.com	www.Transunion.com
800-685-1111	888-397-3742	800-916-8800

- You will be provided with a PIN or password when you place the credit freeze. Keep this information secure to unlock the freeze in the future.
- It's important to note that a credit freeze does not affect your existing accounts, nor does it prevent you from using your credit cards. It only stops new creditors from accessing your credit report.

COMMON TYPES OF FRAUD & SCAMS