EDUCATE YOURSELF
and Stay Informed On Common Fraud Schemes and Tactics

Fraud is the intentional deception of a person or entity by another for personal gain. It benefits everyone to learn how to spot and avoid fraud.

- Stay informed about the latest fraud schemes and tactics used by fraudsters. Familiarize yourself with red flags and warning signs of potential fraud to help you recognize and avoid suspicious activity.
- Visit the Better Business Bureau's BBB Scam Tracker℠ to become familiar with scams in your area.
- The Federal Trade Commission is another great resource. They issue FTC Scam Alerts for common scams nationwide.
- AARP's Scams & Fraud webpage is another great resource.

Follow-Up Actions

☐ PLACE A FRAUD ALERT AND GET YOUR CREDIT REPORTS

- ○ Place a free, one-year fraud alert on your credit report by contacting one of the major credit bureaus (that company must inform the other two).

Equifax	Experian	TransUnion
Fraud Alert	Fraud Alert	Fraud Alert
Security Freeze	Security Freeze	Security Freeze
(800) 685-1111	**(888) 397-3742**	**(800) 680-7289**

- ○ Once an alert has been set up, you'll get a letter from each credit bureau confirming they've placed a fraud alert on your file. Check your credit reports every week for free at AnnualCreditReport.com or call (877) 322-8228 and note any account or transactions you don't recognize.
- ○ When you have an alert on your report, a business must verify your identity before it issues new credit in your name. You can renew the fraud alert after one year.

☐ MONITOR YOUR ACCOUNTS REGULARLY

- ○ Regularly review your statements, transaction confirmations, and credit reports for suspicious activity.
- ○ When possible, set up transaction alerts to be notified when account updates or transactions are processed.

LIMRA LOMA
Navigate With Confidence

☐ UPDATE SECURITY PRACTICES

- ○ Consider using a reputable password manager to create and store strong, unique passwords.
- ○ Regularly update your password and security questions, don't reuse passwords across multiple accounts, and avoid using your email as the username when possible.
- ○ Be cautious of phishing, vishing, and smishing attempts and avoid clicking on suspicious links or attachments.

☐ ENHANCE DIGITAL SECURITY

- ○ Ensure your devices are protected with up-to-date antivirus and anti-malware software.
- ○ Keep your operating systems and applications updated with the latest security patches.
- ○ Avoid using public Wi-Fi for sensitive transactions; use a virtual private network (VPN) if able.

Long-Term Considerations

☐ EDUCATE YOURSELF

- ○ Learn about common phishing scams and other social engineering tactics used by attackers.
- ○ Stay informed about the latest security threats and best practices.

☐ REVIEW AND UPDATE SECURITY POLICIES

- ○ Regularly review and update your security settings on financial and other sensitive accounts.
- ○ Use security features provided by your financial institutions, such as virtual account numbers or transaction limits.

☐ LEGAL AND PROFESSIONAL ADVICE

- ○ Consider consulting with a cybersecurity expert or a legal professional specializing in identity theft and financial fraud for further guidance.