LIMRA and LOMA Consumer Protection Guide

PROTECT YOURSELF
From Fraud Attempts

PROTECT YOURSELF FROM FRAUD ATTEMPTS

- Secure your devices and internet connections:
- Avoid public Wi-Fi networks, which can be easy for hackers to exploit and use to capture your information.
- Never leave your electronic devices unattended in public places.
- A secure website should be identified as "secure" and/or the URL should start with "https." Only give out personal information over a trusted and secure website.

SECURE YOUR ONLINE ACCOUNTS

- Log out of websites and close your web browser when you're finished using them.
- Close or delete any unused accounts with your financial institution(s) and online.

UPDATE YOUR OPERATING SYSTEMS AND ANTI-VIRUS PROGRAM

- Your personal computer will periodically receive updates for your operating system. Always apply them or configure your machine to do it automatically.
- Keep systems and software up-to-date and install a strong, reputable, anti-virus program.

BACK UP YOUR DATA

- Regularly back up your data and verify integrity.
- Whenever you plan to dispose of any old devices, make sure you have deleted all personal information and physically destroy the device when possible.

DON'T STORE SENSITIVE DOCUMENTS IN YOUR EMAIL

- Regularly delete emails from your inbox, sent, and deleted folders.
- Store all sensitive documents such as financial statements, transaction requests, and correspondence with your advisors and financial institutions on your hard drive or in a secure cloud location, not in an email folder.

PROTECT YOUR PHYSICAL DOCUMENTS

- Safeguard physical documents, such as policy statements and correspondence, in a secure location.
- Shred mail and other documents containing sensitive information before disposal.

CHECK YOUR MAIL DAILY

- Avoid leaving outbound or inbound mail in an unsecured mailbox overnight. If you're going to be away from home, place a hold on your mail or have someone you trust collect it daily.

LIMRA LOMA
Navigate With Confidence