GPO FEDERAL CREDIT UNION

4311 Middle Settlement Road • New Hartford, NY 13413
Phone: (315) 724-1654 • Fax: (315) 737-2990 • www.gpofcu.com

IDENTITY THEFT: SENIOR SAFETY

HOW ARE SENIORS TARGETED?

According to the Federal Trade Commission (FTC), people over the age of 60 are more likely to report a tech support scam and less likely to report retail-related scams, especially when they involve financial loss. But there are a variety of scams that specifically target older adults to steal their identity. Some of the most common types of senior identity theft include:

TYPE OF SCAM	ABOUT THE SCAM
Tech support scams	A technical support scam refers to any class of telephone fraud activities in which a scammer claims to offer legitimate technical support service. They may call you, claiming that your software is out-of-date and needs to be replaced. The caller may ask for credit card numbers or for email addresses and passwords to "fix" the problem.
Medicare fraud or other medical identity theft	Someone claiming to be a representative with Medicare or you healthcare provider requests sensitive personal information that's "missing" from your medical records.
IRS scams	Bogus IRS calls typically start to come in around tax time. The caller threatens you with arrest or foreclosure due to back taxes you supposedly haven't paid and demands payment immediately.
Estate identity theft or funeral scams	Fraudsters follow obituaries to steal sensitive information from the deceased, using personally identifiable information such as birth dates, hometowns and any other information they can gather. Scammers may turn up at funerals to take advantage of grieving family members or rob the home while the family is attending services.
Military identity theft	The scammer uses personally identifiable information to take claim of your military benefits, or they contact you claiming to represent the Veterans Administration to request personal information.
Phone scams and robocalls	These callers may want you to claim a free vacation, donate to charity or get a special offer, all with the goal of getting your credit card number and other pieces of personal information.
Grandparent scams	A fraudster calls you, posing as your grandchild in need of help bailing them out of jail in a foreign country or sending money after they were mugged. Of course, your grandchild is safely at home, but if you're not careful, your money could be on its way to a fraudster.
Romance scams	Someone reaches out to you on a dating site and starts chatting. You hit it off, and soon the person is asking for intimate details about you. Suddenly a financial crisis comes up and the person needs you to send money or offer your credit card number. The scammer then disappears with your money and information.

TYPE OF SCAM	ABOUT THE SCAM
Government identification theft	**Social Security number misuse** Call the Social Security Administration (SSA) to report fraudulent use of your Social Security number. As a last resort, you might want to change the number. The SSA will only change it if you fit their fraud victim criteria. You should also order a copy of your Earnings and Benefits statement and check it for accuracy. **Passports** If you have a passport, notify the passport office in writing to be on the lookout for anyone ordering a new passport fraudulently. **Driver's license number misuse** You may need to change your driver's license number if someone is using yours as identification on bad checks. Call the Department of Motor Vehicles (DMV) to see if another license was issued in your name. Put a fraud alert on your license. Go to your local DMV to request a new number. Fill out the DMV's complaint form to begin the fraud investigation process. Send supporting documents with the complaint form to the nearest DMV investigation office. **False civil and criminal judgments** Sometimes victims of identity theft are wrongfully accused of crimes committed by the imposter. If a civil judgment has been entered in your name for actions taken by your imposter, contact the court where the judgment was entered and report that you are a victim of identity theft. If you are wrongfully prosecuted for criminal charges, contact the state Department of Justice and the FBI. Ask how to clear your name.
Banking identity theft	**Dumpster diving** Thieves rummage through trash cans for pieces of unshredded personal information they can use or sell. **Mail theft** Crooks seek out and steal from unattended or unlocked mailboxes to obtain pre-approved credit offers, bank statements, tax forms and convenience checks. **ATM theft or skimming** Thieves secretly attach electronic devices on an ATM to capture numbers when customers swipe their cards. This may include a tiny camera to record the personal identification number (PIN) a customer enters for the transaction. The skimming device may be taped over the card reader. **Imposters** An individual who fraudulently poses as someone who had a legitimate and legal reason to access the victim's personal information (i.e. landlord, an employer, marketer, etc.). **Direct access of personal documents** Unfortunately, there are identity thieves who can gain legitimate access into someone's home and personal information through household work, babysitting, healthcare, friends or roommates, etc. **Purse or wallet theft** Stolen purses and wallets usually contain plenty of bank cards and personal identification. A thief can have a field day using this information to obtain credit under the victim's name or to sell the information to an organized crime ring.

TYPE OF SCAM	ABOUT THE SCAM
Text message scams or SMS phishing (also called smishing)	This occurs when a scam artist uses deceptive text messages to lure consumers into providing their personal or financial information. The scam artist that sends phishing messages often impersonates a government agency, bank or other company to lend legitimacy to their claims. Smishing messages typically ask consumers to provide usernames and passwords, credit and debit card numbers, PINs or other sensitive information that scammers can use to commit fraud. Never provide your personal or financial information in response to text messages from unknown senders. Verify the identity of the sender and take the time to ask yourself why the sender is asking for your information. Contact the business directly by phone and report the text scam.
Online identity theft	**Spyware or malware** Cyber-thieves use a software application that can be remotely installed on your computer with you knowing. This special snoopware lets the thief access everything you do online. Be wary of email attachments and websites you don't know. **Online data** Thieves have purchased sensitive personal information about someone (i.e. name, address, phone numbers, Social Security number, birth date, etc.) from an online broker. **Email fraud and phishing scams** Thieves who appear to be trusted financial institutions use phony emails to hook someone into giving them your financial and personal information.

HOW TO PROTECT YOURSELF

Consider some of the ways you can protect yourself from identity theft. They include:

PROTECTING YOURSELF ONLINE

- Doing business with companies you know and trust. If you haven't heard of the company, research it or ask for a paper catalog before you decide to order electronically. Check with your state consumer protection agency on whether the company is licensed or registered. Fraudulent companies can appear and disappear quickly in cyberspace.
- Checking to see if your computer connection is secure. In Internet Explorer, for example, you should see a small yellow lock in the lower right corner of the screen.
- Using a secure Internet browser that will encrypt or scramble purchase information. If there is no encryption software, consider calling the company's 800 number, faxing your order or paying with a check.
- Never give a bank account, credit card number or other personal information such as your Social Security number and date of birth to anyone you don't know or haven't checked out. Don't provide information that is unnecessary to make a purchase. Even with partial information, con artists can make unauthorized charges to take money from your account. If you have a choice between using your credit card and mailing cash, check or money order, use a credit card. You can always dispute fraudulent credit card charges, but you can't get cash back.

PROTECTING YOUR ATM AND CREDIT CARDS

It is extremely important to protect your personal identification number (PIN). A PIN is a confidential code that is issued to the cardholder to permit access to that account. Your PIN should be memorized, secured and not given out to anyone – even family members or bank employees. The fewer people who have access to your PIN, the better.

- Never write your PIN on ATM cards.

- Don't write your PIN on a piece of paper and place it in your wallet. If your wallet and card are lost or stolen, someone will have everything they need to remove funds from your account.
- Be sure to take your ATM receipt to record transactions and match them against monthly statements. Dishonest people can use your receipt to get your account number.
- Never leave the ATM receipt at the site.
- Avoid providing card and account information to anyone over the phone.
- Only give your credit card account number to make a purchase or reservation you have initiated.
- Never give your credit card to someone else to use on your behalf.
- Watch your credit card after giving it to store clerks to protect against extra imprints being made.
- Destroy any carbons. Don't discard into the trash can at the purchase counter. Keep charge slips in a safe place.
- Save all receipts and compare them to your monthly statement. Report any discrepancies immediately.
- Keep a master list in a secure place at home with all account numbers and phone numbers for reporting stolen or lost cards.
- Use an ATM that is located in an open space with bright lights.
- Be alert. If anything makes you uncomfortable, leave.

FREEZE OR ALERT YOUR CREDIT

Consumers have the right to place a freeze on their credit. Freezing your credit won't hurt your score, but it will keep an identity thief from opening new accounts in your name. A credit freeze does not affect your credit score, but it can keep you from being approved for a new credit card or a loan. A fraud alert, which sounds similar, is not as drastic as a freeze.

To freeze your credit, you will need to report at each credit bureau:

- **Equifax:** 1-800-685-1111 (New York state residents: 1-800-349-9960)
- **Experian:** 1-888-397-3742
- **TransUnion:** 1-888-909-8872