ePAPER

APCI FEDERAL CREDIT UNION

Fighting Identity Fraud

Keep your identity protected

Identity Theft vs. Identity Fraud

Every year thousands of people fall victim to identity theft and identity fraud, yet many cannot differentiate between the two. Despite their similarities, becoming a victim of identity theft or identity fraud has varying impacts on financial well-being and credit. Understanding the differences allows individuals to safeguard themselves and take proactive measures to not fall victim.

Identity theft occurs when someone steals or unlawfully obtains personal, private, or financial information.

There are a variety of ways thieves can steal your identity. Hackers can infiltrate databases, scammers can conduct fraudulent phone calls, criminals can use skimming devices to steal information at point-of-sale terminals, and more. Sometimes, just losing your wallet is enough. When a wallet is stolen it is likely that the thief has access to a person's identification, credit cards, and debit cards.

Identity fraud is the use of stolen personal, private, or financial information for financial gain.

The stolen information can be used for various fraudulent activities such as opening accounts at financial institutions, applying for credit cards or making purchases. The individuals whose identities are stolen, as well as the business owners where fraudulent transactions take place, feel the impact of this crime.

Furthermore, the false identity being used does not always have to belong to a living or genuine individual. Criminals often create fake identities to perpetrate crimes or adopt the identity of someone living or deceased. Falling victim to identity fraud can have a lasting effect on your credit score. Accounts and expenses created by the thieves may stay on your credit report and could become your responsibility until disputed.

There are many ways thieves can use your personal, private, or financial information for financial gain. Some examples of identity fraud include:

- Fake ID or passport
- False credit card accounts
- False accounts at financial institutions
- False loan applications
- Fraudulent withdrawals
- Making unauthorized purchases with stolen information

Personal, private, and financial information should always be kept safe. Be mindful when sharing:

- Full legal name
- Social security number
- Birth date
- Address
- Passwords and PINs
- Credit card numbers
- Account numbers

Popular Fraudster Tactics

Fraudsters will try to obtain personal information through a variety of different tactics. They often use schemes to exploit unsuspecting victims for financial gains. Fraudsters can prey on victims through various means, such as:

- Stealing wallets that contain personal identification information and credit cards.
- Stealing mail from a mailbox or front porch.
- Redirecting mail by submitting a change of address form without the authorization from the intended recipient.
- Scavenging through garbage for personal data.
- Stealing personal identification details from employment records at a workplace.
- Intercepting or otherwise obtaining information transmitted electronically.
- Vishing calls.
- Phishing emails and texts.

Vishing Calls and Phishing Emails

Vishing calls, phishing emails, and phishing texts continue to evolve making it harder to distinguish what is a fraudulent attempt.

In recent cases of vishing calls, fraudsters pose as the fraud department of your financial institution. The fraudster uses technology to spoof the phone number so that the caller ID shows as the intended victim's financial institution. They possess the last four digits of the intended victim's debit card, cite suspicious charges, offer to cancel the card, and send a new one. The fraudster knows and verifies the correct address and phone number(s), and even texts a verification code. In the last part of the scheme, the fraudster asks for the pin number to deactivate the card.

Phishing emails and texts aim to trick recipients into sharing personal information, clicking on malicious links, or opening attachments containing malware. Phishing emails and texts once had errors and poor grammar but have become more sophisticated over time.

Trust your instincts if something seems off. Question whether unexpected calls, emails, or texts could be an attempt to steal your identity to commit fraud.

Best General Practices

1. Safeguard your personal information. Do not share sensitive details, such as social security or account numbers, over the phone unless you are the one who initiated the call and are certain you are dealing with a trustworthy company.
2. Email is not a secure form of communication. Never send personal, private, or financial information in an email.
3. Use strong passwords and never share or reuse usernames, passwords, or PINs.
4. If you are expecting a check order, debit card, or credit card in the mail, and it does not arrive within the window of expected delivery, contact the institution/sender.
5. Do not let mail sit in your mailbox. If you are going to be away from home for more than a day, put a hold on your mail.
6. Lock up any documents that contain personal information. Shred any papers containing personal information before discarding them.
7. Verify that a sender's email address is legitimate before engaging with the email.
8. Monitor your credit reports regularly. Request your free credit report at annualcreditreport.com.
9. Immediately report any suspicious activity on your accounts to the proper authorities.
10. Set up APCI eAlerts for your credit union account so that you are electronically notified when certain events occur within your account.

APCI FCU Protects Your Information

In addition to security factors that are obvious to members, we also practice diligent measures when it comes to our systems that you may not be aware of. This includes regular security updates/patches, strong firewalls, and stringent policies and procedures governing the access of confidential data.

APCI FCU uses various methods to keep your account information safe, including:

- Truncated Account Numbers
- Multi-Factor Authentication (MFA)
- Member Identity Verification