Common Fraud Scams

The **NCUA Fraud Prevention Center** shares key information on common scams, identity theft, and cybercrimes. It is important to be aware of trends and common scams that credit union members may experience.

	Red Flags	**Tips**
Advance-Fee Fraud	• A member urgently requesting a wire transfer internationally who does not have international connections • A member expecting a large financial return following the wire transfer	• Terminate and authenticate communication if you are unsure of its legitimacy and do not share sensitive information or transfer funds
Business and Job Opportunity Scams	• Job and business opportunities that are too good to be true and requests for payment to get the job	• Get a second opinion and take time before accepting a job offer • Research the organization's credentials and ask for the legally required disclosure that outlines any lawsuits against them, the cancellation or refund policy, etc.
Business Email Compromise (BEC)	• Urgent requests for payment, typically via wire transfer	• Check the accuracy of email senders and verify payments with intended recipients • If you detect fraud, contact the originating financial institution
Check Fraud and Check Washing Scams	• The check's intended recipient did not receive it in the mail • Checks that appear altered or damaged • Uncharacteristic check payments to a new payee • Unusual check deposits that are quickly withdrawn or transferred • Reports of lost or stolen checks	• Retrieve your mail regularly and go to your local post office or collection box to deposit outgoing mail • Hold your mail at the post office if you're planning to be away • Maintain appropriate account monitoring and train frontline staff to identify fraudulent checks
Credit and Debit Card Fraud	• Unusual card activity or attempted transactions • Declined transactions	• Perform real-time monitoring and Know Your Customer (KYC) controls to identify unusual transactions
Disaster Fraud	• Requests for money while you are applying for disaster assistance, especially if the requester cannot provide an official ID	• Do not trust anyone or provide personal information without first seeing an official ID • If you suspect fraud, contact government agencies and local law enforcement
Elder Fraud	• Urgency in withdrawing large amounts of money • New relationships or friendships • Sudden and unusual changes to wills	• Perform real-time monitoring and Know Your Customer (KYC) controls to identify unusual transactions and activity • Visit the **Elder and/or Vulnerable Adult Protections topic within InfoSight**.
Fake Check Scams	• You are sent a cashier's check or money order and are asked to send part of the cashed money back in gift cards, money orders, or cryptocurrency	• Do not wire or send gift cards, money orders, or cryptocurrency • Void a check if the amount is more than it should be and request another check for the same amount

Identity Theft	• Unauthorized debit or credit transactions • Personal data discrepancies • Suspicious IDs or documents • Multiple new accounts opened using an existing member's sensitive information	• Verify a business is legitimate before providing sensitive information • Be cautious about what personal data you post to social profiles • Monitor account activity and credit reports regularly • Monitor member transactions for suspicious activity and implement KYC controls to confirm and monitor customer accounts • Visit the **Identity Theft topic within InfoSight.**
Imposter Scams	• Requests for personal or financial info or money transfers	• Government agencies will not ask for sensitive information or payment – terminate and authenticate any communications if you are unsure
Internal Fraud	• Employees living beyond their means; with family or financial problems; who are unusually close with a vendor or member; addicted to drugs, alcohol, or gambling • Employees with excessive or unusual wire transfer activity • Customer or vendor reports of missing funds or payments	• Conduct pre-employment screening and background checks on prospective employees • Implement internal controls such as four-eyes checks, (require two people to verify certain transactions), segregation of duties, and mandated vacations • Regularly perform internal and external audits
Investment Fraud	• Promises of high returns with no risk along with high-pressure sales tactics	• Do independent research, consult with fiduciary financial advisors, or talk with people you trust before investing • Report any suspected fraud to the applicable agencies (SEC, FINRA, CFTC, FBI, FTC)
Invoice Fraud	• Unusual changes in payment or account details • Discrepancies in vendor information and bank account details	• Implement strict procedures for invoice payments • Establish regular communications with vendors and track invoice activity • Match invoices with purchase orders and confirm payment information • Implement internal controls such as four-eyes checks
Loan Fraud	• Inconsistent financial information on loan applications • Mismatch between the borrower profile and intended purchases • Collateral value discrepancies	• Implement due diligence checks and other fraud controls and build them into policies and procedures • Conduct post-payment assurance work to identify and recover any fraud losses
New Account Opening Fraud	• Suspicious documents • Large cash deposits • Inconsistent transactions	• Implement strong KYC controls and real-time behavioral and transaction monitoring
Online Shopping Scams	• An order that did not arrive and/or a denied refund request • Unauthorized credit and debit card transactions	• Read refund and return policies before purchasing • Dispute charges for orders that did not arrive and denied refund requests • Use a credit card for online purchases • Use official retailer websites and apps • Monitor card transactions for unauthorized activity

Ponzi and Pyramid Schemes	• A consistent flow of unregistered investments • A business that does not sell a legitimate product and lacks sales revenue	• Implement strong KYC controls and real-time behavioral and transaction monitoring
Prizes, Sweepstakes, and Lotteries	• Communication claiming you won a prize, lottery, or sweepstakes that you did not enter, followed by a request for money or account information to cover the upfront taxes and fees • Pressure and/or sense of urgency to act quickly	• Do not send money or provide personal information if you did not enter the lottery or sweepstakes • Terminate and authenticate communication if you are unsure
Ransomware	• Unusual emails, including an increase in spam emails and phishing attempts	• Use anti-virus and anti-malware programs to perform system and software scans • Make an offline backup of your data • Update operating systems and software frequently
Romance Scams	• Requests for money for emergencies or for personal information from someone you have not met in person	• Be careful what you share on social profiles and do not send money, gifts, or gift cards to someone you have not met in person • Reverse image search someone if you suspect them to be
Spoofing & Phishing	• Slightly tweaked email addresses or website URLs, mimicking a trusted source, such as changing a letter, symbol, or number • Generic greetings and/or signatures • Misspellings, inconsistent formatting, poor sentence structure and grammar issues • Requests for sensitive info for verification purposes • Pressure to open and download attachments	• Verify a source is legitimate before clicking on any links or downloading anything from emails or messages • Hang up on any calls from unknown callers requesting information • Do not provide sensitive information if the request is unsolicited over the phone or internet • Install cybersecurity measures such as anti-virus software and firewalls
Technical Support Impersonation Scams	• Emails received regarding unsolicited services, pressuring you to act quickly	• Do not give others full control access to your computer or send wire transfers to unknown entities, and do not download software from them
Wire Fraud	• *Changes in established payment or account details* • *Unusual wire transfer activity* • *Transactions initiated online or through mail*	• *Implement a detection system with real-time monitoring to identify and prevent wire fraud*