Fraud Scams: Quick Reference Guide

Nasdaq Verafin

This quick reference guide is designed to help those combating fraud within financial institutions learn about common scam scenarios. Feel free to share this page with front-line staff, colleagues, and peers.

SCAM	DEFINITION	VICTIMS	INDICATORS
Authorized Push Payment (APP) Fraud	A customer is manipulated into transferring funds to a fraudster, who is posing as a genuine payee.	Victims may be businesses or consumers, depending on the form of APP fraud.	• See Business Email Compromise, Romance Scams, and Investment Scams
Business Email Compromise (BEC)	Criminals send an email message that appears to come from a known source making a legitimate request.	Large corporations, small businesses, and organizations such as financial,commercial, non-profit, non-governmental, or government institutions.	• Transfers initiated near the end-of-day (or cut-off windows) and/or before weekends or holidays. • Large wire or funds transfer to a recipient the company has never dealt with previously. • Name of the receiving account is the same or similar to payments sent in the past, but the routing details are different. • Receiving account does not have an established history of receiving payments. • Receiving account is a personal account and the company typically only sends wires to other businesses.
Romance Scam	A criminal adopts a fake persona to gain a victim's trust and uses the illusion of a romantic relationship to manipulate the victim into sending them funds or account information, or making transactions on the criminal's behalf.	All demographics can fall victim to romance scams. While seniors are often victimized, predators are also using these scams to target youth and teens.	• Funds transfers to international locations. • Funds transfers to crypto exchanges. • Large ATM withdrawals. • Client uncharacteristically using lines of credit or pulling from investments. • Large purchases at locations that process funds transfers.
Investment Scam	A scammer uses the promise of low or zero-risk investments and guaranteed future returns to lure victims into sending payments.	Anyone can fall victim to an investment scam, though individuals looking to grow their wealth may be more at risk.	• Funds transfers to international locations. • Funds transfers to crypto exchanges. • Clients pulling funds from unusual sources and transferring the funds.
Financial Grooming *("Pig Butcher-ing")*	A scammer convinces a victim to purchase a cryptocurrency investment by promising a high return. The investment opportunity is fake, and the funds are stolen.	While anyone can fall victim to financial grooming, individuals in financial need may be more susceptible.	• Client with no history of using virtual currency attempts to purchase large amounts of virtual currency. • Client liquidating savings and attempting to wire the proceeds to a VASP or convert the funds to virtual currency.
Advanced Fee Fraud	A fraudster promises something highly valuable in exchange for a relatively small upfront fee, which they steal — leaving the victim with nothing in return.	Victims vary depending on the form of advanced fee fraud that is used.	• See lottery scams and online and payday loan scams.
Lottery Scam	Lottery scams promise large lottery winnings in return for an initial processing fee from the victim.	Victims are typically elderly persons, and those who may be financially vulnerable.	• Large funds transfer that is not typical for the client. • Funds transfers to international locations. • Large ATM withdrawals. • Large purchases at locations that process funds transfers, such as big box stores and international wire processors. • Client using lines of credit or pulling from investments, which is out of character for them.

Fraud Scams: Quick Reference Guide *continued*

Nasdaq Verafin

SCAM	DEFINITION	VICTIMS	INDICATORS
Online & Payday Loan Scam	A fraud targeting individuals with the promise of a loan in exchange for a fee.	Victims are often individuals with poor credit history or difficulty obtaining a loan.	• Mobile deposits or payments that are new or not typical for the client. • Immediate withdrawal or transfer of funds from the account. • Large purchases at locations that process funds transfers.
Elder Scam	A senior transfers money to a stranger or imposter for a promised benefit or good that they do not receive.	Scammers are especially interested in seniors who are high wealth, may be isolated or have cognitive challenges.	• Older client appears frantic and mentions needing to send funds urgently for an emergency. • Older client making uncharacteristic financial decisions and cannot be contacted. • Older client making frequent large withdrawals, especially from dormant accounts, and attempting to initiate high-value wires or purchase large numbers of gift cards.
Employment Scam	A fraudster poses as a potential employer, convincing victims to process financial transactions, or forward them money or personally identifiable information.	Anyone can be a victim, but job seekers such as college students or those seeking employment as a caregiver, or a work-from-home job may be especially targeted.	• New clients or clients who are financially vulnerable. That is, with little access to credit, no or inconsistent payroll, and/or those with a low dollar balance in their account. • Mobile deposits or payments that are new or not typical for the client. • Immediate withdrawal or transfer of funds from the account. • Large purchases at locations that process funds transfers.
Disaster Scam	A fraudster exploits tragedy to defraud their victims, often capitalizing on relief efforts after a natural disaster or other catastrophe to steal personal information and funds.	Victims are typically those seeking relief after a disaster.	• Deposits of multiple emergency assistance checks or electronic funds transfers into the same account. • Cashing of multiple emergency assistance checks by the same individual. • Opening of a new account with an emergency assistance check, where the name of the potential account holder is different from that of the check depositor. • Transactions where the payee organization's name is similar to, but not exactly the same as, those of reputable charities. • The use of money transfer services for charitable collections.
Health Scam	A fraudster targets individuals or the family of individuals with ailing health, taking advantage of their stress and desperation to sell phony health products or steal personally identifiable information.	Victims are typically individuals or the family of individuals with a serious health issue, such as addiction, dementia, diabetes, COVID-19, or cancer.	• Merchant's website has a name/web address similar to real and well-known companies, a limited internet presence or a location outside of the United States. • Merchant requests payments that are unusual for the type of transaction or unusual for the industry's pattern of behavior. • Merchant claims several last minute and suspicious delays in shipment or receipt of goods.
Family Emergency Scams	A customer is manipulated into sending funds to a fraudster posing as a family member in crisis.	Primarily family members and/or friends of the individual being imitated.	• Client appears frantic and mentions needing to send funds urgently for an emergency. • Large, uncharacteristic payment(s) through an irreversible payment method, such as a wire or ACH transfer. • Large payments to a suspicious or offshore account. • First-time crypto activity.

CONTACTS

Fraud/Compliance contact: ____________________

Police: ____________________

Other: ____________________

NOTES

____

____

____