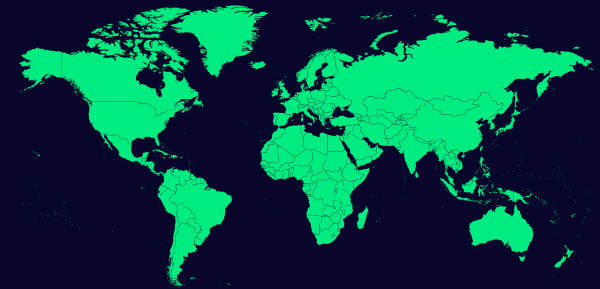


Understanding Fraud Schemes & Scams

A guide to common scenarios used by fraudsters to victimize your customers.



In 2023 consumer
fraud scams caused

\$43.6B
in losses globally,
shouldered by everyday people
and businesses with potentially
life changing consequences.¹

Source

¹ 2024 Nasdaq Global Financial Crime Report



Table of Contents

Introduction	1
--------------------	---

SECTION 1

Authorized Push Payment Fraud	2
1.1 Business Email Compromise	3
1.2 Romance Scams	4
1.3 Investment Scams.....	5
1.4 Financial Grooming	6

SECTION 2

Advanced Fee Fraud	7
2.1 Lottery Scams	8
2.2 Online & Payday Loan Scams.....	9

SECTION 3

Elder Scams	10
-------------------	----

SECTION 4

Employment Scams.....	11
-----------------------	----

SECTION 5

Disaster Scams	12
----------------------	----

SECTION 6

Health Scams	13
--------------------	----

SECTION 7

Family Emergency Schemes	14
--------------------------------	----

FIGHTING SCAMS

A New Era of Fraud	15
The Human Impact of Fraud Schemes	16

JOB AID

Fraud Scams Quick Reference Guide	17
-----------------------------------------	----



Fraud is constantly evolving, and the losses are immense.

As the industry has implemented controls to protect against traditional first-party and account takeover fraud, fraudsters have adjusted their strategies to focus on your customers to help facilitate the attack.

This has spawned an ever-increasing number of scams across various payment channels targeting consumers and businesses alike. While fraud scams have been around for some time, they continue to evolve as fraudsters adjust to the changing payments landscape.

In the fight against fraud, it is critical to understand the key components of fraud scams, such as victimology, key indicators, and opportunities for mitigating risk. This book, based on numerous industry sources and Nasdaq Verafin's decades of experience in financial crime management, is designed to help you identify the characteristics of common fraud scams.

Authorized Push Payment Fraud

What is it?

In authorized push payment (APP) fraud, a customer is manipulated into transferring funds to a fraudster, who is posing as a genuine payee.² Business Email Compromise, romance scams, and investment scams are all forms of APP fraud.

Who are the victims?

Victims may be businesses or consumers, depending on the form of APP fraud. For example, fraudsters target individuals with romance scams, and corporate customers with Business Email Compromise.

How does it work?

APP fraud can be extremely lucrative, with a devastating impact on those targeted. While the exact tactics depend on the form of APP used, victims are typically manipulated into making a payment under false pretenses, such as purchasing non-existent goods, or transferring funds into an account under criminal control in response to an urgent but fictitious request.²

APP fraud can be particularly challenging to detect as the authorized customer initiates the payment, rendering most authentication-based controls, such as tokens and one-time passwords, ineffective.

Source

² APP scams, Payment Systems Regulator, 2022



Business Email Compromise

What is it?

Criminals send an email message that appears to come from a known source making a legitimate request.³

Who are the victims?

Targets include large corporations, small businesses, as well as organizations such as financial, commercial, non-profit, non-governmental, or government institutions.¹

How does it work?

Business Email Compromise (BEC) was linked to \$6.7 billion in losses globally in 2023.¹ In these scams, fraudsters send an email urgently requesting a transfer of funds or other valuables, such as gift cards,³ or asking for changes to payment instructions. In some cases, they may use targeted techniques (e.g., spear phishing, spoofing email accounts or websites, or using malware) to access corporate systems first, before making their requests.



Victims of BEC scams are typically convinced that the transaction is for legitimate business reasons, with fraudsters timing their activities and infiltrating email chains to make their requests appear authentic.³

Source

¹ 2024 Nasdaq Global Financial Crime Report

³ Business Email Compromise, FBI, 2022

What are the indicators?

- **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.

How to mitigate the risks?

- **Callback procedures** for certain fund transfer types.
- **Targeted training** of key financial officers for your business and corporate clients.
- **Training for internal staff** (Account Managers, BSA, Fraud, Wire Room, etc.) to identify BEC.
- **Transaction monitoring** that profiles both sending and receiving accounts of a funds transfer to ensure the activity is typical for both parties.

Romance Scams

What is it?

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,⁴ or making transactions on the criminal's behalf.⁵

Who are the victims?

All demographics can fall victim to romance scams. While seniors are often victimized,⁶ predators are also using these scams to target youth and teens.⁷

How does it work?

In 2023, romance scams caused \$3.8 billion in global losses with other confidence schemes.¹ In these scams, the fraudster will contact the victim through social media networks, online forums, or dating sites, often taking several months to build trust. While typically located overseas, the fraudster may portray themselves as an American (military, business professional, etc.).⁸

At some point the fraudster will initiate and escalate requests for money, claiming they need the funds for travel expenses to see the victim, emergency medical expenses, a business opportunity, or another fictitious purpose. The fraudster may also request online login details with a plan to gain access to the victim's accounts.⁸

Victims may be used as an unwitting money mule, moving funds for the fraudsters—without realizing they are laundering the profits of other crimes.¹

Sources

¹ 2024 Nasdaq Global Financial Crime Report

⁴ Romance Scams, FBI, 2022

⁵ Money Mules: A Financial Crisis, IC3, 2021

⁶ Internet Crime Report, FBI, 2021

⁷ Scams are targeting teenagers. Here's how to keep your kids safe., Washington Post, 2023

⁸ Cyber Actors use Online Dating Sites to Conduct Confidence/Romance Fraud and Recruit Money Mules, IC3, 2019

What are the indicators?

- Funds transfers to international locations.
- Funds transfers to crypto exchanges.
- Large ATM withdrawals.
- Client using lines of credit or pulling from investments, which is out of character for them.
- Large purchases at locations that process funds transfers, such as big box stores and international wire processors.

How to mitigate the risks?

- Training front-line staff to identify escalating funds transfers to a relatively new recipient—especially if located overseas.
- Detection systems that profile both sending and receiving accounts of a funds transfer to ensure the activity is typical for both parties.

Investment Scams

What is it?

A scammer uses the promise of low or zero-risk investments and guaranteed future returns to lure victims into sending payments.⁹

Who are the victims?

Anyone can fall victim to an investment scam, though individuals looking to grow their wealth may be more at risk.

How does it work?

Fraudsters will use a variety of methods to target their victims, leveraging online ads and forums, in-person seminars, phone calls, or online dating apps.



Scammers use strategies to gain the trust of the victim, relying on false testimonies and “patented” methods of success, often asking for money upfront — to maximize the investment.

Scammers will then defraud their victims, often asking for continued investments that never come to fruition.⁹ Cryptocurrency is often exploited in investment scams, with schemes such as financial grooming a major concern.

Source

⁹ Business and Investment Fraud, FBI, 2022

What are the indicators?

- Funds transfers to international locations.
- Funds transfers to crypto exchanges.
- Clients pulling funds from unusual sources and transferring the funds.

How to mitigate the risks?

- Training for front-line staff to identify escalating funds transfers to a relatively new recipient — especially if located overseas.
- Detection systems that profile both sending and receiving accounts of a funds transfer to ensure the activity is typical for both parties.

Financial Grooming

Also known as “Pig Butchering”

What is it?

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.

Who are the victims?

While anyone can fall victim to financial grooming, individuals in financial need may be more susceptible.

How does it work?

Fraudsters typically contact victims through text message, social media or dating sites claiming they dialed a wrong number or are trying to reconnect with an old friend. After establishing rapport, the fraudster pitches an investment opportunity to the victim that involves cryptocurrency and promises exceptional returns.¹⁰ After obtaining an initial investment, the scammer will share fake evidence of immense returns and ask for more funds to invest. As the funds are transferred, they are siphoned into accounts under criminal control.¹⁰ This continues until the victim has no more to give, at which point the fraudster disappears with all the funds.¹⁰



Many scammers refer to financial grooming as “Pig Butchering” after the process of fattening a hog for slaughter, and the stages of the scam, where victims’ assets are gathered and eventually drained.¹⁰

Source

¹⁰. FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as “Pig Butchering”, FIN-2023-Alert005, 2023

What are the indicators?

- 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.

How to mitigate the risks?

- Training for front-line staff to identify individuals who mention a new contact referring them to a lucrative investment opportunity involving virtual currency.
- Detection systems that identify unusual logins from unique IP addresses, geographic locations and more.
- Detection systems that profile both sending and receiving accounts of a funds transfer to ensure the activity is typical for both parties.
- Detection systems that identify first-time crypto activity, involving wires destined for known crypto endpoints or a crypto recipient, that may be uncharacteristic for your customer and indicative of a potential crypto-related scam.

Advanced Fee Fraud

What is it?

A fraudster promises something highly valuable in exchange for a relatively small upfront fee, which they steal—leaving the victim with nothing in return. Examples include lottery scams and online and payday loan scams.

Who are the victims?

Victims vary depending on the form of advanced fee fraud that is used. For example, individuals facing financial difficulties may be more susceptible to lottery or online and payday loan scams.

How does it work?

A scammer claims to have access to something incredibly valuable, such as millions of dollars, an exceptional loan opportunity or a service that will eliminate the victim's financial debt. The scammer offers these valuables to the victim in exchange for a nominal fee, usually justified as a membership cost, taxes, or shipping and handling, that must be paid in advance.¹¹



After receiving the funds, the scammer disappears or requests further fees from the victim, who never gains anything in return.

Source

¹¹. Types of Consumer Fraud, Office of the Comptroller of the Currency, N.D.



Lottery Scams

What is it?

Lottery scams promise large lottery winnings in return for an initial processing fee from the victim.¹²

Who are the victims?

Victims are typically elderly persons, and those who may be financially vulnerable.

How does it work?

Fraudsters will use mass phishing techniques to identify victims and lure them in with the prize of a large lottery win.



Victims are requested to forward a processing fee to the fraudster before receiving their winnings.

If the victim does forward a fee, then the fraudster will make additional requests for funds — often under the guise of withholding tax fees or administration fees. This will continue until the victim catches on or runs out of money.

Source

¹². Sweepstakes, Lottery, and Prize Scams, International Association of Better Business Bureaus, 2020

What are the indicators?

- 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.

How to mitigate the risks?

- Training for front-line staff to identify individuals who are excited/happy about making a large transfer. Client may say they just won the lottery or have come into unexpected money.
- Detection systems that profile both sending and receiving accounts of a funds transfer to ensure the activity is typical for both parties.

Online & Payday Loan Scams

What is it?

A fraud targeting individuals with the promise of a loan in exchange for a fee.¹³

Who are the victims?

Victims may be individuals with poor credit history or difficulty obtaining a loan.¹³

How does it work?

Fraudsters may contact victims online, or even by posting ads in newspapers and magazines. These ads promise access to loans regardless of credit history or employment status.¹³



Once the victim responds, the fraudster may request financial details from the victim such as account information or online/mobile login credentials.

They then use this information to either initiate ACH credits or perform mobile deposits to the account with instructions for the victim to then return a portion of the funds as part of a processing fee.

In another version of the scam, criminals request an urgent and upfront insurance or application fee, then break off contact with the victim once the payment is made.¹³

Source

¹³. What To Know About Advance-Fee Loans, FTC, 2022

What are the indicators?

- **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**, such as big box stores and international wire processors.

How to mitigate the risks?

- **Real-time detection capabilities** for incoming payments across multiple payment channels.
- **System to review and compare check images** to identify unusual deposited items.

Elder Scams

What is it?

A senior transfers money to a stranger or imposter for a promised benefit or good that they do not receive.¹⁴

Who are the victims?

Scammers are especially interested in seniors who are high wealth, may be isolated or have cognitive challenges.¹⁴

How does it work?

In 2023, of all reported global fraud, \$77.7 billion was linked to elderly victims.¹ Fraudsters often target older adults who they may perceive as isolated, less familiar with technology, challenged by disability, and generally more vulnerable.

Scammers may impersonate a person in a position of trust or extort funds through fear tactics. In grandparent schemes, another example of a financial crime targeting seniors, a scammer impersonates the victim's grandchild requesting financial aid in a crisis.



Seniors who are exploited often do not report the crime to authorities out of shame, uncertainty of who to turn to, or simply a desire to leave the event behind. But the experience often leaves them with lasting consequences and trauma.

Source

¹ 2024 Nasdaq Global Financial Crime Report

¹⁴ Advisory on Elder Financial Exploitation, FIN-2022-A002, 2022

What are the indicators?

- 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.

How to mitigate the risks?

- Training for front-line staff to identify older adults who appear distressed regarding their financial accounts and may be instructed by someone else, especially by phone.
- Detection systems that segment wires by sender type for more targeted analysis based on the specific fraud risks and scams for elderly persons.
- Detection systems that identify first-time crypto activity, involving wires destined for known crypto endpoints or a crypto recipient, that may be uncharacteristic for your customer and indicative of a potential crypto-related scam.

Employment Scams

What is it?

A fraudster poses as a potential employer, convincing victims to process financial transactions, or forward them money or personally identifiable information.¹⁵

Who are the victims?

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.¹⁶

How does it work?

Scammers may pose as legitimate employers by spoofing company websites and posting fake job openings on popular online job boards. They then conduct false interviews with unsuspecting applicants, from whom they eventually request personally identifiable information or funds.¹⁵



Criminals may use the victim's financial information to initiate ACH credits or perform mobile deposits to the victim's account. They then instruct the victim to forward the funds into an account they control, less a fee that is meant as payment.

In other cases, the fraudster will pretend to overpay the victim with fake checks and request that the difference be returned with a wire transfer, or open accounts in the victim's name using personally identifiable information stolen earlier in the scam.

Sources

¹⁵ FBI Warns Cyber Criminals Are Using Fake Job Listings to Target Applicants' Personally Identifiable Information, FBI El Paso, 2021

¹⁶ Job Scams, FTC, 2020

What are the indicators?

- **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**, such as big box stores and international wire processors.

How to mitigate the risks?

- **Account opening procedures probing for possible employment scam scenarios** (i.e., Why are you choosing our institution today?).
- **Real-time detection capabilities** for incoming payments across multiple payment channels.
- **System to review and compare check images** to identify unusual, deposited items.

Disaster Scams

What is it?

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.

Who are the victims?

Victims are typically those seeking relief after a disaster.¹⁷

How does it work?

Disaster fraudsters thrive on the urgency, anxiety, and desperation in the wake of a disaster. They may pose as contractors, government officials, or other individuals in a position of trust, demanding upfront payment for work they claim is urgent, but ultimately never complete. In other cases, they may solicit donations to an illegitimate charity and pocket the proceeds.¹⁸



Criminals will often demand payment through irrevocable or anonymous payment methods, such as wire transfers, or cryptocurrency and gift cards. They may also request bank account information or Social Security Numbers.¹⁹

In some cases, fraudsters will attempt to obtain relief funds for which they are not entitled, depositing emergency assistance checks, or receiving payment by wire transfer. The funds are then immediately withdrawn.

Sources

¹⁷ Charity and Disaster Fraud, FBI, 2022

¹⁸ Advisory to Financial Institutions Regarding Disaster-Related Fraud, FIN-2017-A007, 2017

¹⁹ Scammers target disaster victims. Spot their traps. FTC 2022

What are the indicators?

- **Deposits of multiple emergency assistance checks** or electronic funds transfers into the same bank 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.**

How to mitigate the risks?

- **System to review and compare check images** to identify unusual, deposited items.
- **Detection systems that profile both sending and receiving accounts of a funds transfer** to ensure the activity is typical for both parties.
- **Monitoring of online banking activity** to detect unusual access to customers' online accounts.

Health Scams

What is it?

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.²⁰

Who are the victims?

Victims are typically individuals or the family of individuals with a serious health issue, such as addiction, dementia, diabetes, COVID-19, or cancer.^{20, 21}

How does it work?

A fraudster advertises a product they claim will help individuals afflicted with an illness. The product is often presented as a cure-all, and may feature testimonials of miraculous benefits, fabricated scientific language and claims that the product is backed by prestigious awards, such as the Nobel Prize. The victim, desperate to help themselves or their family, purchases the product, and the fraudster steals the funds and their personally identifiable information. If the victim does receive a product, it may provide no health benefits, or worse, even endanger their health.²⁰

Sources

²⁰. Common Health Scams Federal Trade Commission Consumer Advice, 2022

²¹. Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19), FIN-2020-A002, 2020

What are the indicators?

- **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.

How to mitigate the risks?

- **Behavior-based analytics that evaluate a customer's transaction along with their historical patterns of activity** to accurately detect anomalous activity.
- **Detection systems that profile both sending and receiving accounts of a funds transfer** to ensure the activity is typical for both parties.

Family Emergency Schemes

What is it?

A customer is manipulated into sending funds to a fraudster posing as a family member in crisis.

Who are the victims?

Primarily family members and/or friends of the individual being imitated.

How does it work?

Fraudsters pose as a customer's family member and request emergency transfers for various emergencies, from being stranded without access to funds²² to needing payment for ransom fees.²³

While fraudsters traditionally relied on fraudulent phone calls, their own acting abilities and the power of suggestion for these scams, virtual kidnapping is an evolution of the fraud where bad actors use deepfake technology to exact funds from victims with ultrarealistic videos.

Fraudsters will pose as a family member in distress and ask for ransom money, usually through an irrevocable payment method such as a wire or ACH transfer. The victim later finds out their family member was never in danger. The deepfake makes the scam feel authentic — and enhances the scammer's ability to manipulate their target.

Widespread use of social media allows fraudsters to make these scams even more effective. If a target's family member posts photos or videos of themselves on vacation, fraudsters may use this as intelligence to make their scam more believable.



Virtual kidnapping is an ultrarealistic form of family emergency scam where AI-generated videos of a loved one held hostage are used to exact funds for ransom.

Sources

²² Scammers Use Fake Emergencies to Steal Your Money, FTC, 2023

²³ FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions, FinCEN, 2024

What are the indicators?

- **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.
- **Large payments** to a suspicious or offshore account
- **First-time crypto activity.**

How to mitigate the risks?

- **Training for front-line staff to identify customers who appear distressed** regarding their financial accounts and may be instructed by someone else, especially by phone.
- **Detection systems that segment wires by sender type** for more targeted analysis based on the specific fraud risks and scams for elderly persons.
- **Detection systems that identify first-time crypto activity**, involving wires destined for known crypto endpoints or a crypto recipient, that may be uncharacteristic for your customer and indicative of a potential crypto-related scam.

A New Era of Fraud

Fraud is evolving. Scammers are abusing new technology to improve their scams while moving quickly to exploit new vectors and different victim demographics. In turn, financial institutions must keep up with the frenetic pace of change.

Generative artificial intelligence (AI) and deepfake technology have enabled a surge of increasingly bold scams, such as virtual kidnapping. For those who fall prey, the consequences are financially and psychologically devastating.



Deepfake: A video, photo, or audio recording that has been manipulated with AI to resemble someone else. The technology can create, edit and replace faces, and synthesize speech.

Fraudsters are also sharing best practices and technology with each other to democratize their scams. Fraud-as-a-service models and tools distributed on the dark web make it easy for criminals to initiate sophisticated schemes such as Business Email Compromise.

The constant evolution of technology and fraud scams mean that financial institutions' role in prevention has never been more important. Through effective knowledge and tools, the industry can safeguard our financial system and communities today and tomorrow.

“Vigilance by financial institutions to the use of deepfakes, and reporting of related suspicious activity, will help safeguard the U.S. financial system and protect innocent Americans from the abuse of these tools.”

– Andrea Gacki, *FinCEN Director, 2024*





The Human Impact of Fraud Schemes

The monetary consequences of fraud scams often overshadow their very real impacts on everyday people. Regardless of age, demographics, or profession, no one is immune — and many victims lose their livelihoods and experience lasting trauma. Individuals can experience these effects directly, such as romance scam victims who often face psychological, emotional, and even physical harm, or indirectly such as BEC severely impacting the reputation and growth of an organization, jeopardizing the career and earnings of its employees. No dollar value can capture this toll. It is immeasurable — and preventable.

Working directly with customers and members, financial institutions are a crucial front-line defense against fraud schemes and scams. Your dedication to tactful inquiry, vigilance for red flag indicators, having effective fraud controls in place, and timely reporting to law enforcement is essential to protect victims from the devastating human consequences of these financial crimes.

“ Losing the money was obviously devastating. But what’s worse is what it does to your heart, your trust. ”

- Debby Montgomery Johnson, *Victim of Romance Scam*¹

“ Don’t assume it can’t be you. No matter what you do for a living, or where you are in your life or how efficient you think you are — nobody is above being scammed. ”








- Lilah Jones, *Victim of Business Email Compromise*¹

Source







¹ 2024 Nasdaq Global Financial Crime Report

Fraud Scams: Quick Reference Guide

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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Funds transfers to international locations. • Funds transfers to crypto exchanges. • Clients pulling funds from unusual sources and transferring the funds.
 Financial Grooming ("Pig Butchering")	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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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*

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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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



Nasdaq Verafin provides cloud-based Financial Crime Management Technology solutions for Fraud Detection, AML/CFT Compliance, High-Risk Customer Management, Sanctions Screening and Management, and Information Sharing.

More than 2,600 financial institutions globally, representing nearly \$10T in collective assets, use Nasdaq Verafin to prevent fraud and strengthen AML/CFT efforts.

Leveraging our unique consortium data approach in targeted analytics with artificial intelligence and machine learning, Nasdaq Verafin significantly reduces false positive alerts and delivers context-rich insights to fight financial crime more efficiently and effectively.

To learn how Nasdaq Verafin can help your institution fight fraud and money laundering

Visit: **www.verafin.com**

Email: **info@verafin.com**

Call: **1.877.368.9986**

Legal **www.nasdaq.com/legal**

© 2024 Nasdaq Verafin Inc. All rights reserved.

Updated Q1, 2025