VERAFIN
A STEP AHEAD

Understanding Fraud Schemes & Scams

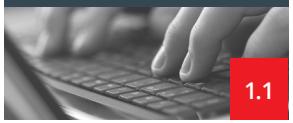
A guide to common scenarios used by fraudsters to victimize your customers.

Updated Q4 2022

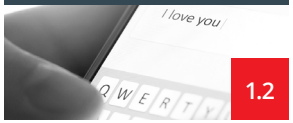
Sections

AUTHORIZED PUSH PAYMENT FRAUD

BUSINESS EMAIL COMPROMISE

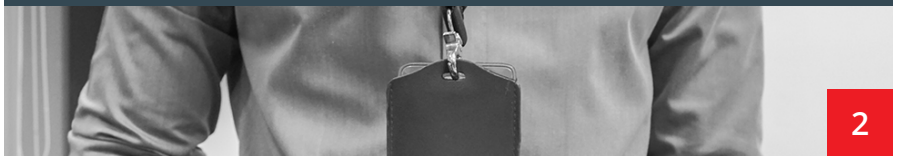


ROMANCE SCAMS



INVESTMENT SCAMS

EMPLOYMENT SCAMS



ONLINE & PAYDAY LOAN SCAMS

DISASTER SCAMS

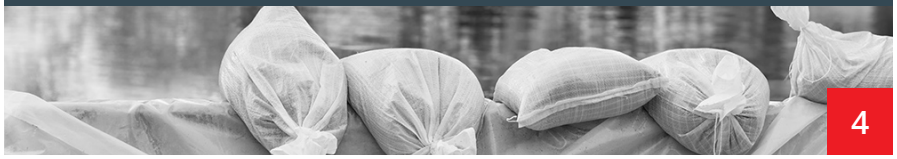


TABLE OF CONTENTS

Updated November 2022

Introduction

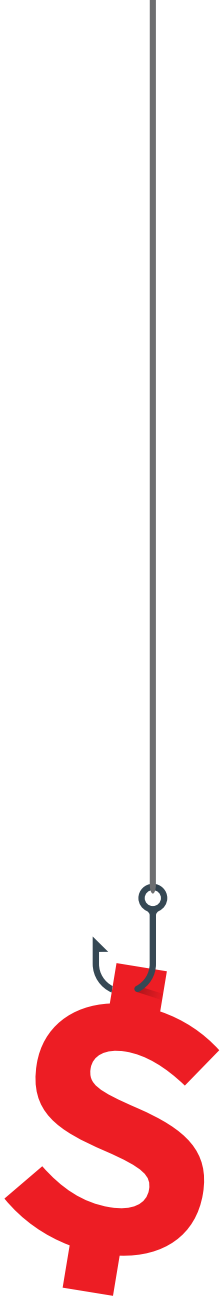
Fraud is constantly evolving.

As the industry has implemented controls to protect against traditional first-party fraud 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 Verafin's decades of experience in financial crime management, is designed to help you identify the characteristics of common fraud scams, including:

- Authorized Push Payment Fraud, such as:
  - » Business Email Compromise
  - » Romance Scams
  - » Investment Scams
- Employment Scams
- Online & Payday Loan Scams
- Disaster Scams



SECTION 1

Authorized Push Payment (APP) Fraud

What is it?

In APP fraud, a legitimate customer is manipulated into transferring funds to a fraudster, who is posing as a genuine payee.[1] 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.[1]

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.

Resources

1. APP scams, Payment Systems Regulator, 2022

SECTION 1.1

Business Email Compromise (BEC)

What is it?

Criminals send an email message that appears to come from a known source making a legitimate request.[2]

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.[2]

How does it work?

Fraudsters send an email urgently requesting a transfer of funds or other valuables, such as gift cards,[2] 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]

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.

Resources

2. Business Email Compromise, FBI, 2022
3. Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes, FIN-2019-A005, 2019

SECTION 1.2

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?

While all demographics can fall victim to romance scams, seniors are most often targeted.[6]

How does it work?

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.).[7]

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, or alternatively, convince the victim to transfer fraudulent funds as an unsuspecting money mule.[5,7]

Increasingly, romance scammers are also exploiting cryptocurrency to defraud their victims, such as convincing their victims to convert funds at a cryptocurrency ATM to take advantage of blockchain anonymity.[6]

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 processers.

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.

Resources

4. Romance Scams, FBI, 2022
5. Money Mules: A Financial Crisis, IC3, 2021
6. Internet Crime Report, FBI, 2021
7. Cyber Actors use Online Dating Sites to Conduct Confidence/Romance Fraud and Recruit Money Mules, IC3, 2019

SECTION 1.3

Investment Scams

What is it?

A scammer uses the promise of low or zero-risk investments and guaranteed future returns to request an upfront payment.[8]

Who are the victims?

Anyone can fall victim to an investment scam, though seniors are often targeted.[8]

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.[8]

Cryptocurrency is being increasingly exploited in investment scams, with schemes such as *Pig Butchering* a major concern. In a *Pig Butchering* scheme, criminals convince their victims to make repeated apparent cryptocurrency investments, preying on the general lack of understanding surrounding digital currency. The invested funds are ultimately siphoned into accounts under criminal control.[9,10]

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.

Resources

8. Business and Investment Fraud, FBI, 2022
9. Cryptocurrency Investment Schemes, IC3, 2022
10. FBI Oregon Tech Tuesday: Building a Digital Defense Against a New Cryptocurrency Scam: Pig Butchering, FBI Portland, 2022

SECTION 2

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.[11]

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.[12]

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.[11]

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.

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 processers.

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.

Resources

11. FBI Warns Cyber Criminals Are Using Fake Job Listings to Target Applicants' Personally Identifiable Information, FBI El Paso, 2021
12. Job Scams, FTC, 2020

SECTION 3

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 are often individuals with poor credit history or difficulty obtaining a loan for a variety of reasons.[12]

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.[14]

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.[12]

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 processers.

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.

Resources

13. What To Know About Advance-Fee Loans, FTC, 2022
14. Predatory Loans and Loan Scams, New York State Department of Financial Services, No Date

SECTION 4

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.[15]

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 individual 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.[16]

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.[17]

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.

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 depositer.
- **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.

Resources

15. Charity and Disaster Fraud, FBI, 2022
16. Advisory to Financial Institutions Regarding Disaster-Related Fraud, FIN-2017-A007, 2017
17. Scammers target disaster victims. Spot their traps. FTC 2022

Fighting Fraud Scams:
The Power of Consortium Analytics

Consortium analytics are a powerful approach to fraud prevention. By leveraging information from thousands of financial institutions to profile hundreds of millions of counterparties, they allow your institution to truly understand the risk associated with both sides of a transaction.

You gain insights into whether a payee has a trusted history of activity, or is a likely mule account opened to facilitate fraud — and as payments are identified as fraudulent, detected mule accounts are recognized in any future analysis for all financial institutions who are members of the consortium.

With fraudsters constantly refining their scam tactics and targeting victims across America, conventional detection approaches cannot keep pace with the evolving financial crime landscape today, and there is significant risk in relying on these approaches in the future. Through the power of consortium analytics, Verafin's robust Financial Crime Management platform provides exceptional detection for payments channels commonly exploited in fraud scams, such as wire. Leveraging the profiles of 300 million counterparties based on our consortium of 2200 financial institutions, combined with cross-channel intelligence and real-time analysis, you gain the ability to confidently identify high-risk payments destined for potential mule accounts and shut down suspicious transfers before the funds leave your institution. Our approach also provides the added benefit of allowing safe payments to proceed uninterrupted, lowering the operational costs of alert reviews and customer call-backs.

To learn more about how Verafin can effectively protect your financial institution and customers with consortium analytics, download our Payments Fraud Product Brochure.

Fraud Scams: Quick Reference Guide

VERAFIN
A STEP AHEAD

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. Business Email Compromise, romance, and investment scams are all forms of APP fraud.	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.*	While all demographics can fall victim to romance scams, seniors are most often targeted.	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 request an upfront payment.*	Anyone can fall victim to an investment scam, though seniors are often targeted.	Funds transfers to international locations. Funds transfers to crypto exchanges. Clients pulling funds from unusual sources and transferring the funds.
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.
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.
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 depositer. 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.

CONTACTS

FRAUD/COMPLIANCE CONTACT: _____

POLICE: _____

OTHER: _____

OTHER: _____

NOTES

_____

_____

_____

_____

Verafin is the industry leader in enterprise Financial Crime Management solutions, providing a cloud-based, secure software platform for Fraud Detection and Management, BSA/AML Compliance and Management, High-Risk Customer Management and Information Sharing.

More than 3500 banks and credit unions use Verafin to effectively fight financial crime and comply with regulations.

Leveraging its unique big data intelligence, visual storytelling and collaborative investigation capabilities, Verafin significantly reduces false positive alerts, delivers context-rich insights and streamlines the daunting BSA/AML compliance processes that financial institutions face today.

Verafin is the exclusive provider for Texas Bankers Association, Western Bankers Association, and CUNA Strategic Services, with industry endorsements in 48 U.S. states.

For more information, contact Verafin today.

1.877.368.9986
info@verafin.com
www.verafin.com

VERAFIN
A STEP AHEAD