



FRAUD PREVENTION & AWARENESS: ANTI-SCAM INDUSTRY WORK EFFORT

This publication provides a concise, practical overview of the latest scam trends impacting the payments industry and offers actionable strategies to detect, prevent, and respond to scam-based fraud. With input from across the payments ecosystem, it aims to educate stakeholders, empower consumers, and strengthen systemic fraud mitigation efforts.

Table of Contents

Understanding Scams

- Scam Definition & Payment related scope
- Changing Tactics & Red Flags
- Best practices for consumers

Mitigation Strategies

- Issuers
- Acquirers
- Business & Organizations

Technology in Scam Prevention

- Technology Levers
- Prevalent & Evolving Tools

Client Reminders & Resources

What is a scam?



“the use of deception or manipulation intended to achieve financial gain”.¹

¹<https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/scams/scamclassifier-model/>

Scope: Payment card-related Scams



All scams originate with deception and manipulation: they exploit human nature



The financial gain can be obtained through many channels: e.g. payment cards, wire, and ATMs









Mitigation efforts can differ by channel



This discussion will focus on card-related scams, though the recommendations may apply to multiple types of payments

Scammers stories may change but red flags stay the same

Red Flags:

-  **Contacted unexpectedly** with a request to provide payment or personal information
-  **Pressured to act quickly** or given an urgent deadline
-  **Asked to pay in unusual ways** such as gift cards or wire transfers to “protect” your money
-  **Offered something** that sounds too good to be true
-  **Told NOT to speak** to others about the situation (keeping it confidential)
-  **Someone you’ve never met** in person quickly builds a connection on social media and asks for help

Scammers stories may change but red flags stay the same

Scammers will:

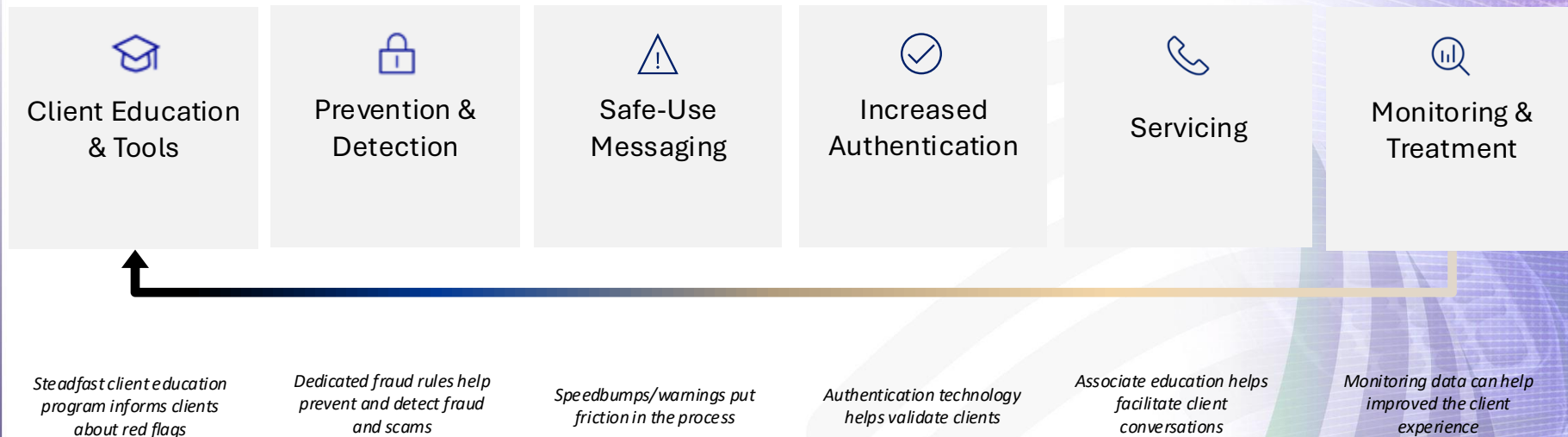
- Play on emotions and use stories that invoke feelings of fear, greed, sympathy, or love and urge you to ignore your instincts
- Pretend to be from a trusted company or organization & claim there's a serious problem needing immediate action
- Ask for personal or business info or money or try to coach you through steps that give them access to your devices or accounts
- Trick you into sharing verification codes
- Spoof phone numbers to make it seem like they're calling from a real company
- Imitate official websites or e-mail addresses to look legit (like irs.com instead of the real irs.gov)

Scammers stories may change but red flags stay the same

Consumers should:

- ✓ **Not let anyone rush** them into a decision. Scammers push urgency because it works.
- ✓ **Pause** and **Verify requests** are legitimate - contact merchants or organizations directly. Ask themselves if the request makes sense? (i.e. did they use a toll, are they expecting a package?)
- ✓ **Set up transaction alerts** and customize for your activity with dollar limits and transaction types
- ✓ **Avoid clicking or downloading** links or attachments
- ✓ **Not send gift cards or money** to someone they met online
- ✓ **Financial Institutions will never ask consumers to move money**, withdraw cash, or deposit to a new account to “fix” an issue or “protect your money”
- ✓ **Never provide remote access** at someone’s request
- ✓ **Never ignore scam warning messages** – they exist to protect you

Mitigation techniques for issuers: Need an end-to-end approach



Scam Prevention for Issuing Financial Institutions



Use technology/tools to monitor transactions in real-time to analyze transaction patterns and alert, block, or decline suspicious activity

- Payments data analytics and reporting
- Machine learning algorithms
- Behavioral analytics



Educate customers on common scams and prevention methods

- Scam warnings that disrupt; pop-ups or text box warnings during risky transaction attempts
- Tailored messages that sound direct, empathetic, and conversational



Scam Intake and Dispute Flow

- Implement a claim intake/dispute process flow that distinguishes between fraud, scams, and merchant disputes
- Use scripting that helps clients identify scams without shame ("Were you pressured or convinced to make this payment vs. Were you scammed?")



Empathy training for employees

- Train employees to recognize scams and provide customer support without blame

Scam Mitigation Techniques for Acquirers



Acquirers and their merchant-facing partners, ISOs and agents, have both direct and indirect ability to mitigate fraud, whether it originates from [scams](#) or other sources. Higher fraud leads to higher chargebacks, which can lead to penalties and even merchant account closures.



Since scams arise from “[the use of deception or manipulation](#)”, mitigating their impact involves both educating consumers or employees and using technology to delay suspect payments, and encouraging the payor to be doubly sure whom they are paying.



Technology allows monitoring payment endpoints and flagging activity that is atypical or unrecognized. This should be combined with communication to the payor, recommending verification of the payee.



Proper risk monitoring, specifically use transaction velocity checks to monitor newly onboarded merchants. Upon detection of suspect activity, consider suspending merchant’s settlement funding until properly investigated.



This information will most likely originate from acquiring financial institutions and/or their direct ISO partners and will be passed on to those (e.g., sub-ISO, agents, PayFacs) who have a direct relationship with merchants.

Scam Prevention for Businesses / Organizations

For Internal Risks
(committed by
employees to perpetrate
scams)

- Prevent unauthorized access by employees:
 - Set appropriate entitlements
 - Track access and inquiries through alerts and user logs
 - Restrict data extraction
 - Encrypt data

For External Risks
(targeting employees)

- Prevent phishing or social engineering of employees:
 - Require multi-factor authentication for employee network to mitigate compromised credentials due to scams
 - Conduct phishing email training and testing for all employees
 - Provide training to employees on data security and scam risks

Technology levers to prevent scams

Because scams and classic fraud both leave abnormal footprints on the same payment rails, the core technology stack to detect, interrupt, and contain is similar



Detect Unusual Activity

Continuously watch for behavior or transaction patterns that don't fit a customer's or merchant's normal profile, then raise a flag in real time.



Protect Sensitive Data

Store and move payment information in ways that make it useless if intercepted or mis-used, so deception alone can't unlock spendable data.



Force a Pause or Additional Confirmation

Introduce an extra moment of confirmation whenever risk looks elevated, giving the sender time to rethink and break the scammer's "act now" pressure.



Identify Suspicious Parties

Whether it's a fraudster using stolen credentials or a scammer setting up shell accounts, controls like KYC (Know Your Customer), digital ID verification, and synthetic identity detection can block suspect actors from accessing the financial system.

Prevalent Technology to Help Address Payment Scams

Prevalent Technology	Issuers	Acquirers	Merchants	Processors / Gateways
Real-time Anomaly Screening: Flags unusual transactions instantly using rules or ML at key points in the payment flow	✓	✓	✓	✓
Multi-factor authentication (OTP / 3-DS / passkeys): Adds a second factor so stolen or coerced credentials alone won't succeed	✓		✓	
Fraud alerts & customer notifications: Instant warnings give cardholders a chance to stop or question suspicious transactions	✓			
Tokenization (card-on-file / network tokens): Replaces the real PAN with a valueless token, neutralizing data-theft pay-offs	✓	✓	✓	✓
AVS & CVV matching: Confirms billing address and security code in card-not-present purchases		✓	✓	✓
3-D Secure / secure-checkout delegation: Shifts risky e-commerce orders back to the issuer for step-up verification	✓	✓	✓	✓
Charge-back management & issuer alerts: Early-warning workflows help claw back funds from scam-triggered disputes	✓	✓	✓	
Encryption & PCI-compliant data handling: Protects card data in transit and at rest, closing many compromise routes	✓	✓	✓	✓
Compliance tooling (PCI-DSS, AML, sanctions): Automated controls enforce scheme rules and legal checks before funds move	✓	✓		✓
Transaction aggregation & portfolio monitoring: Dashboards reveal macro anomalies or coordinated scam rings	✓	✓		✓
Address & identity verification (KYC / KYB): Confirms customer or business identity against trusted data sources	✓	✓	✓	✓

Evolving Technology to Help Address Payment Scams

Evolving Technology	Issuers	Acquirers	Merchants	Processors / Gateways
Behavioral Analytics & Biometrics: Monitors interaction patterns to detect bots, coercion, or abnormal user behavior	✓		✓	
Adaptive & Context-Aware Authentication: Dynamically adjusts user verification steps based on risk signals	✓		✓	
Neural-network & deep-learning scoring: High-dimensional AI spots subtle, cross-channel scam indicators	✓	✓	✓	✓
Digital-ID & synthetic-identity detection: Real-time validation blocks fabricated identities at onboarding	✓	✓		✓
AI-driven identity graphs: Cross-entity link-analysis reveals hidden connections between accounts, devices, addresses			✓	✓
Seamless biometric payments (face / fingerprint): Low-friction yet strong authentication in app or POS			✓	
AI-driven dynamic routing (smart auth hops): Sends each transaction through the optimal risk-/cost path		✓		✓
Automated KYC for merchant onboarding: Instant doc & liveness checks stop shell merchants used in scams		✓		✓
AI “fraud-orchestration” engines: Central hub picks the best fraud tool set per transaction in real time		✓		✓
Data Collaboration & Analytics: Industry-wide intelligence sharing across payment ecosystem participants.	✓	✓		✓
Blockchain / ledger traceability pilots: Immutable ledgers streamline tracing and claw-back of scam funds				✓
API-first / micro-services architecture: Modular stack enables rapid plug-in of new anti-scam capabilities		✓	✓	✓

Reminders for Consumers to Avoid Scams

Stay vigilant and take proactive steps to protect against scams

Be Skeptical of Unsolicited Communications

- Avoid clicking on unknown links or attachments
- Verify unexpected phone calls, emails or text messages are legitimate
- If you're being asked to act fast; SLOW DOWN, take a pause

Verify the Source

- Check official websites to verify a request directly with the merchant / organization
- Use the phone number on your card or statement to contact the bank or merchant

Protect Personal Information

- Don't share sensitive info without verifying the request is legitimate
- Enable multi-factor authentication (MFA) to access your accounts

Use Strong, Unique Passwords

- Use a password manager
- Avoid password reuse

Educate Yourself

- Stay updated on scam tactics

Secure Your Devices

- Install antivirus and anti-malware software
- Use data encryption
- Update software regularly

Be Cautious with Public Wi-Fi

- Avoid sensitive transactions on public Wi-Fi
- Use a VPN for added security

Resources for Consumers

Resources:

Federal Trade Commission (FTC) - <https://reportfraud.ftc.gov/>

Helps protect consumers from scams, fraud, by providing education, investigations & place to report scams

Internet Crime Complaint Center (IC3) - <https://www.ic3.gov/>

Helps consumers report online crimes like scams, fraud, cyberattacks.

Identity Theft Resource Center (ITRC) - <https://www.idtheftcenter.org/>

Free resources for identity theft victims, including toolkits, hotlines, and recovery plans

Better Business Bureau Scam Tracker – <https://www.bbb.org/scamtracker>

Track scams, check scam reports, or share your experience

AARP Fraud Watch Network – <https://www.aarp.org/fraudwatchnetwork>

Articles, scam alerts, a help line (877-908-3360) for all, and events tailored for seniors and caregivers

Local Police Department

Important if money was lost or identity was stolen. A police report may be needed for recovery steps

Bank, Credit Union, or Financial Institution

Immediately notify your bank to stop payment, freeze accounts, or investigate scam payment activity

Elder Justice Hotline: 1-833-Fraud-11 (or 833-372-8311)

Victims aged 60 or over who need assistance filing an IC3 Complaint or with other resource needs can call for assistance. (MF 10A-6P EST)

Thank You!

If you have any questions about the content in this resource,
please reach out to info@uspaymentsforum.org.



www.uspaymentsforum.org



Legal Disclaimer

This document is provided solely as a convenience to readers, as a high-level overview of strategies commonly used to help increase awareness of and protect against scam-based fraud. The strategies, technologies and other considerations described herein do not represent an exhaustive list, and effective security practices and strategies depend on and should be tailored to an organization's specific needs, risk profile, and other factors. The information herein does not constitute legal advice, and all warranties of any kind, express or implied, are expressly disclaimed.

Readers interested in securing against scam-based fraud should consult their respective security providers, business partner, subject matter experts and professional and legal advisors prior to any implementation decisions.