Mastering the Warning Signs: Red Flag Training For Frontline and Back Office Teams on Wires, ACH, and Check Fraud

STOUT

AGENDA

- Overview
- Red Flags
- Best Business Practices

Overview

Fraud is evolving quickly- so must your strategy!

What are the latest fraud trends?

- **Fraud as a Service (FaaS)** - Cybercrime is becoming more commercialized every year, with fraud automation and phishing kits available for purchase similar to a monthly description
- **Credential Stuffing** - Fraudsters are increasingly leveraging software or bots to test stolen or leaked credentials at scale.
- **SMS phishing** - The frequency of SMS phishing attacks targeting customers is exploding. As email clients become more sophisticated at detecting and stopping phishing attacks, fraudsters are turning to a channel with far fewer spam controls: SMS. SMS messages are also many times more likely to be opened than email, making SMS an increasingly attractive channel for scammers.
- **AI-Powered Deepfake Scams** - Fraudsters are increasingly using generative AI to create realistic deepfake audio and video, enabling them to impersonate bank officials or customers. These sophisticated scams have led to significant financial losses
- **Synthetic Identity Fraud** - Criminals are combining real and fabricated information to create synthetic identities, which are then used to open fraudulent accounts. This type of fraud is particularly challenging to detect.

Check Scams

Check fraud occurs when an unauthorized person uses someone else's checks, or images of a check, to make unauthorized purchases or withdrawals.

- Overpayment scam
- Fake Payment for Sold Goods
- Remote Deposit Fraud
- Counterfeit Checks
- Check Washing/ Alterations

Business Email Compromise

Business Email Compromise (BEC) is a sophisticated and highly targeted form of cybercrime where attackers exploit email systems to deceive individuals or organizations into transferring money or sensitive information. These scams often involve impersonation and social engineering tactics.

How BEC Works

- Impersonation: Cybercriminals pose as trusted individuals, such as executives, vendors, or partners, using spoofed or hacked email accounts.
- Deception: They craft convincing messages to request urgent payments, sensitive data, or changes to payment details.
- Execution: Victims, believing the request is legitimate, comply, resulting in financial or data loss.

Business Email Compromise

Common BEC Scenarios

- Attackers impersonate a company executive to request wire transfers.
- Fraudsters pose as suppliers and request payment to a fraudulent account.
- Criminals trick HR or payroll departments into redirecting employee salaries.
- Attackers request sensitive employee or customer data for further exploitation.

Crypto-Currency Scams

Cryptocurrency investment fraud, which the media commonly describes as "pig butchering," is one of the most common and damaging fraud scams.

- Victim Selection
- Build Trust
- The Pitch
- The initial investment
- The “growing’ investment
- Taxes, fees and the end of the scam

Account Takeover

Account takeover, also known as ATO, is a form of identity theft in which a malicious third-party gains access to or “takes over” an online account. Cyber criminals may gain access to a victim’s online account through a variety of methods:

- Brute Forcing username/password
- Phishing emails
- Phishing domains/websites
- Social engineering data breaches
- Malware

Fraud detection is crucial for financial institutions as it protects assets, maintains customer trust, and ensures compliance with regulations, ultimately safeguarding the institution's reputation and financial stability.

Red Flags

Red Flags in Wire Transfers

- Unusual or urgent wire requests from customer or internal employees.
- Changes to beneficiary information without proper verification.
- Source of funds is unusual or has incorrect recipient information.
- High-value transactions with unfamiliar recipients.

Red Flags in ACH

- Sudden changes in ACH file patterns (e.g., unusual volume, amounts, or recipients).
- Unauthorized ACH debits or credits.
- Discrepancies in payroll files or vendor payments.
- Account takeover attempts (e.g., login from suspicious IP addresses).
- Unusual timing
- Behavior during verification

Red Flags in Checks

- Altered or counterfeit checks (e.g., mismatched fonts, irregular signatures).
- Duplicate check numbers or amounts that don’t match customer history.
- Payee name discrepancies.
- Checks presented for payment after account closure.

Best Business Practices

Team Responsibilities

- **Frontline Teams**: Recognizing red flags during customer interactions and transaction initiation.
- **Back Office Teams**: Monitoring for anomalies, verifying suspicious transactions, and escalating concerns.
- **Collaboration:** Importance of communication between frontline and back-office teams to ensure comprehensive fraud detection.

Frontline Check Fraud Mitigation

- **Check Stock Quality:** Check for perforations, paper thickness and security features like watermarks or special inks. Fragile paper or missing security features could indicate a counterfeit check.
- **Payee Name Verification:** Ensure the payee name matches the entity presenting the check. Be skeptical of generic names or abbreviations.
- **Payor Name and Address:** Ensure that the issuer's information is consistent with known details. Unknown payor names and P.O. boxes could be red flags.
- **MICR Line:** Validate that the information is clean, formatted correctly, and properly aligned. Check for unusual fonts, spacing issues, smudged or shiny ink, or bumpy surfaces.
- **CAR/LAR Mismatch:** Confirm that the numerical and legal amount (written) match exactly. Any differences should be alerted immediately.
- **Signature Verification:** Ensure that the signature on the check matches what is on file. Signature mismatches could indicate forgery.
- **Endorsements:** Verify the accuracy of the endorser's signature on the back of the check. Check for signs of forgery or alterations.
- **Check Numbers and Dates:** Check numbers appear both in the upper right corner and are represented within the MICR line - and they must match. Also, be aware of stale-dated and post-dated checks.
- **Physical Signs:** Be skeptical of checks with different ink colors, difficult to read writing, chemical changes, erasures, and look for fade spots on the paper.

Tools and Resources

- Fraud Detection Systems
- Policies and Procedures
- Training Programs
- Regular reviews of transaction patterns, customer profiles, and system settings.
- Call-back verification for wire instructions.
- Cross-checking transaction details with known customer profiles.
- Escalation processes for suspicious transactions

Responding to Red Flags

- Immediate Actions: Steps to take when a red flag is detected (e.g., freezing transactions, escalating to management).
- Escalation Processes: Who to notify and how to document concerns.
- Customer Communication: Handling fraud concerns professionally while safeguarding relationships.

Training Techniques

Microlearning

- Deliver short, focused lessons (3-10 minutes) on specific topics like fraud detection, customer service, or compliance.
- Staff can complete quick sessions during breaks or downtime without feeling overwhelmed.
- Example: A 5-minute video or infographic on identifying counterfeit checks or spotting fraud red flags.

Interactive Scenarios

Use real-world examples or role-playing to simulate situations staff face daily, such as handling suspicious transactions or difficult customers.

Mimics their actual work environment, making training relevant and actionable.

Example: A mock scenario where staff must verify an urgent wire transfer request or request to deposit a suspicious item.

All Fun and Games

Incorporate game elements like quizzes, challenges, or leaderboards into training to make it engaging and competitive.

Adds fun and motivates staff to participate actively.

Example: A fraud detection challenge where staff compete to identify the most red flags in a transaction.

Visual Learning Aids

Use posters, infographics, or quick-reference guides displayed in work areas to reinforce training concepts.

Provides easy, ongoing access to key information without requiring formal training time.

Example: A flowchart on steps to escalate suspicious activities or a checklist for verifying wire transfers.

Rewards and Recognition

Recognize staff who excel in applying training concepts, such as fraud prevention or customer service.

Motivates staff to engage with training and reinforces positive behavior.

Example: Awarding a "Fraud Prevention Hero" badge for identifying and stopping a suspicious transaction.

Focused Training Checklist

Provide concise checklists for essential tasks, like verifying transactions or handling compliance issues.

Simplifies complex processes and ensures consistency in execution.

Example: A checklist for escalating suspicious ACH requests or verifying check authenticity.

About Stout

What We Do

PAYMENT SERVICES

- ACH, Remote Deposit Capture, Wire Transfer, Treasury Program Services.
- Risk assessments and full scope audits
- Support services for financial institution FinTech relationships
- Payment Services Enhancement Projects
- Payments Training

FINANCIAL CRIMES SERVICES

- Fraud system implementation and optimization
- Fraud program buildout
- Fraud management program documentation (e.g., policy, procedures, processes)

FINTECH COMPLIANCE AND TECHNOLOGY

- Assessment and redesign of operating platforms
- Compliance advisory documentation services

PROCESS IMPROVEMENT, EFFICIENCY, ENHANCEMENT, AND SYSTEM SUPPORT

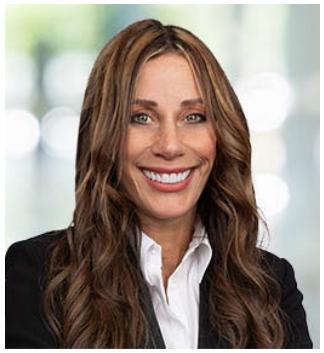
- Policy and procedures updates for newly implemented systems
- Risk management
- Organizational structure strategies and implementation
- Operational improvement services

CORE CONVERSION SUPPORT SERVICES FOR FINANCIAL INSTITUTIONS

Conversion leadership, e.g., task and timeline management, calls with vendors, onsite support for test week and conversion “Go Live” and post conversion support

RISK MANAGEMENT MEMBERSHIP - https://simplifyrisk.stout.com

Who We Are



Terri Sands, CAMS- Audit, AAP, CFE
Managing Director, Regulatory Compliance, Payments and Financial Crimes
tsands@stout.com
Office: +1.678.573.2693

Kelly Rozier, AAP APRP
Manager
krozier@stout.com
Office: +1.404.369.1143

Stout is a global advisory firm specializing in corporate finance, accounting and transaction advisory, valuation, financial disputes, claims, and investigations. We serve a range of clients, from public corporations to privately held companies in numerous industries. Our clients and their advisors rely on our premier expertise, deep industry knowledge, and unparalleled responsiveness on complex matters.

https://simplifyrisk.stout.com