# Supplement to Key Findings from the Annual Federal Reserve Financial Services (FRFS) Financial Institution Risk Officer Survey (2024)

THE FEDERAL RESERVE
Financial Services

# Table of Contents

## About the Risk Officer Survey

This annual survey was conducted by Federal Reserve Financial Services (FRFS), a collaboration of the 12 Federal Reserve Banks, and requested responses from senior risk experts at institutions using financial services offered by FRFS. FRFS provides payment services including cash, check, ACH, funds transfer and instant payments to financial institutions. Accordingly, the research, statements and findings contained in this summary are not independent academic research. Readers should look at a variety of sources when assessing the potential insights to both the payments industry level and their various organizations, rather than relying on any single source. The insights are more helpful when looking across multiple years. The sampling margin of error is +/- 6% at a 95% confidence level. FRFS provides several tools to support institutions in supplementing their internal tools to further help identify and/or mitigate payments risk.

## About the Supplement

This supplement extends the 2024 Risk Officer Survey Key Findings by providing detailed segment analysis of fraud and scam experiences across different financial institution types and asset sizes. It offers enhanced visualizations of previously published FraudClassifier model data while introducing new insights from the ScamClassifier model. The segmentation analysis reveals how banks and credit unions of varying sizes experience different patterns of fraud events and scam types, allowing for more targeted risk management strategies. By highlighting segment-specific vulnerabilities, this supplement enables financial institutions to better understand how fraud and scam trends affect their market segment(s). These granular insights support more effective fraud prevention planning tailored to institution type and size.

## Executive Summary

The 2024 Risk Officer Survey reveals significant patterns in fraud and scam experiences across financial institutions of varying types and sizes. Physical forgery/counterfeit (63%), physical alteration (51%) and digital payment fraud (51%) emerge as the most prevalent and persistent fraud events overall. Banks report higher vulnerability to physical fraud types, while credit unions face greater challenges with compromised credentials and digital payment fraud. Institution size also impacts fraud exposure, with smaller institutions (<$100M) primarily confronting digital payment fraud, mid-sized institutions ($100M-$1B) struggling with physical forgery and alteration, and larger institutions experiencing both physical forgery and compromised credentials challenges.

In scam typology, romance impostor scams represent the most significant and growing threat across institution segments. Trust-based scams — including romance, bank impostor and family/friend schemes — pose challenges, with banks specifically concerned about romance and business impostor scams. Credit unions similarly prioritize romance scams but also highlight "other trusted party" scams as significant threats. These findings emphasize the need for targeted fraud prevention strategies that address the specific vulnerabilities of each institution type and size segment.

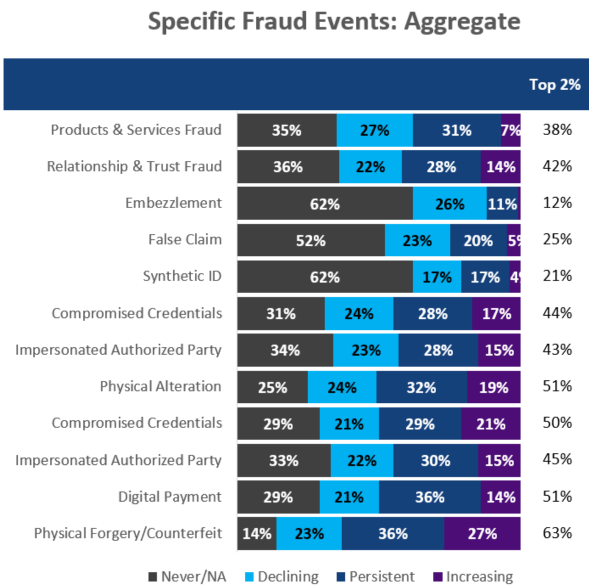
Would you like more information about fraud and scam information? Staci.Shatsoff@bos.frb.org.

Do you have ideas, questions, or want to learn more about the survey? Robert.A.Williams@chi.frb.org.

# Chart 1

Chart 1 expands on the visualization of chart five from the [Key Findings report (PDF)]() by including bank and asset sizes to help highlight differences in these market segments. The percentages shown represent the top two selections — those reflecting increasing and persistent responses of events.

## Specific Fraud Events by Segment




**Specific Fraud Events: Peer Segment Benchmarks**

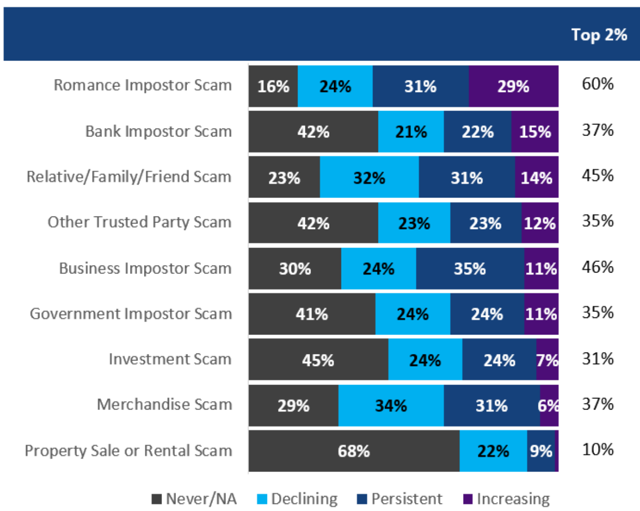
| | Total | Bank | CU | <$100M | $100M - $1B | $1B+ |
|---|---|---|---|---|---|---|
| Products and services fraud | 38% | 37% | 40% | 13% | 33% | 51% |
| Relationship and trust fraud | 42% | 42% | 46% | 17% | 43% | 49% |
| Embezzlement | 12% | 10% | 20% | 9% | 10% | 14% |
| False claim | 25% | 22% | 37% | 17% | 21% | 32% |
| Synthetic ID | 21% | 17% | 43% | 4% | 14% | 36% |
| Compromised credentials | 44% | 44% | 49% | 17% | 38% | 61% |
| Impersonated authorized party | 43% | 42% | 46% | 9% | 38% | 59% |
| Physical alteration | 51% | 55% | 34% | 17% | 54% | 58% |
| Compromised credentials | 50% | 50% | 51% | 26% | 44% | 64% |
| Impersonated authorized party | 45% | 45% | 46% | 17% | 39% | 62% |
| Digital payment | 51% | 50% | 51% | 35% | 46% | 61% |
| Physical forgery/counterfeit | 63% | 66% | 49% | 26% | 64% | 74% |

1. In total fraud events, physical alteration (51%), digital payment (51%) and physical forgery/counterfeit (63%) were among the fraud events most experienced and viewed as persistent and growing.
2. Banks reported physical forgery/counterfeit (66%) and physical alteration (55%) as the leading fraud events within their institutions. Credit unions were affected most by compromised credentials (51%) and digital payment fraud (51%).
3. Across asset sizes, institutions under $100M saw digital payment (35%), compromised credentials (26%) and physical forgery (26%) as most prominent. Institutions between $100M and $1B saw physical forgery/counterfeit (64%) and physical alteration (54%) as the leading fraud events, and the largest institutions most prevalently faced physical forgery/counterfeit (74%) and compromised credentials (64%).

## Chart 2

Utilizing the ScamClassifier model,* financial institutions indicated romance impostor scams as their most experienced and increasing scam. Percentages displayed in the right-hand chart represent the top two selections — those reflecting increasing and persistent responses of experienced events.

### Specific Scam Events by Segment




**Specific Scam Events: Peer Segment Benchmarks**

| | Total | Bank | CU | <$100M | $100M - $1B | $1B+ |
|---|---|---|---|---|---|---|
| Romance impostor | 60% | 60% | 59% | 14% | 68% | 63% |
| Bank impostor | 37% | 37% | 41% | 14% | 33% | 49% |
| Relative/family/friend | 45% | 44% | 50% | 38% | 46% | 47% |
| Other trusted party | 35% | 31% | 53% | 19% | 32% | 44% |
| Business impostor | 46% | 47% | 38% | 14% | 46% | 55% |
| Government impostor | 35% | 35% | 32% | 5% | 35% | 43% |
| Investment | 31% | 29% | 35% | 10% | 30% | 37% |
| Merchandise | 37% | 37% | 38% | 38% | 37% | 36% |
| Property sale or rental | 10% | 10% | 15% | 0% | 7% | 17% |

1. Trust-related scams, such as romance impostor (29%), bank impostor (15%), and relative/family/friend scams (14%), are viewed as increasing and the most challenging for financial institutions.
2. Banks saw romance impostor (60%) and business impostor (47%) scams as top concerns, while credit unions saw romance impostor (59%) and other trusted party scams (53%) as their most significant challenges.
3. Based on asset sizes, smaller financial institutions are most concerned with relative/family/friend (38%) and merchandise scams (38%). Financial institutions with assets between $100M and $1B saw romance impostor (68%), relative/family/friend (46%), and business impostor scams (46%) as most pressing. Larger financial institutions similarly saw romance (63%) and business impostor scams (55%) as critical.

*See page 8 for detailed questions.*

## Resources

### FRFS Ancillary Risk Tools Available to Financial Institutions

- Risk Management Toolbox (FRBServices.org®)
- FedDetect® Notification Services, including Duplicate Check Notification, FedACH® Anomaly Notification and Payee Name Verification
- Check: Advanced Notice Return Report: FedPayments® Reporter Service for Check Services
- ACH: FedPayments Insight Service for FedACH Services
- ACH: FedACH Risk® Management Services
- Funds Transfer: FedTransaction Analyzer®
- Instant Payments: Network-level limits, participant-level limits, and negative lists
- Instant Payments: Managing Fraud Risk – FedNow® Service Readiness Guide
- Instant Payments (New Mid-2025): Account activity thresholds
- Exception Management: Exception Resolution Service

### Industry Collaboration

- FraudClassifier Model
- About the ScamClassifier Model
- Collaboration is Key — The Importance of Information Sharing (PDF)
- Synthetic Identity Fraud Mitigation Toolkit
- Scams Mitigation Toolkit

## Respondent Profile (362 responses)

| | | | |
|---|---|---|---|
| Bank | 77% | Assets Over a Billion | 36% |
| Credit Union | 23% | Assets $100M - $1 Billion | 47% |
| Service Provider | <1% | Assets Under $100M | 14% |
| | | Bankers' Banks, Foreign Banks, and Service Providers | 3% |

## Detailed Questions and Available Selections

**Chart 1:** How often have your institution and account holders experienced the following types of fraud events during the past 12 months? *(Available selections: Do not know or not applicable, Never, Experienced but declining, Experienced and persistent, Experienced and increasing)*

**Chart 2:** How often have your institution and account holders experienced the following scam types during the past 12 months? *(Available selections: Do not know or not applicable, Never, Experienced but declining, Experienced and persistent, Experienced and increasing)*

# Definitions

### Check Fraud Types

| | |
|---|---|
| **Paperhanging** | Intentionally writing bad checks |
| **Kiting** | Timing check deposits to get the cash before it bounces |
| **Float** | Trying to time the float on a check |
| **Payee forgery** | Payee name altered |
| **Endorsement forgery** | Endorsing and depositing a check |
| **New account opening** | Opening new account with a fraudulent check |
| **Washing** | Chemically altering the check |
| **Counterfeit check** | Printing up checks using stolen data |

### FraudClassifier Model Definitions

| | | |
|---|---|---|
| **Manipulated authorized party** | Products and services fraud | Paid for product/service never delivered or grossly inferior to what was promised (e.g., lottery scams, travel scams) |
| | Relationship and trust fraud | Funds transferred to trusted party or imposter without expectation of services (e.g., IRS scams, romance scams) |
| **Authorized party acted fraudulently** | Embezzlement | Theft or misuse of employer funds or trustee fiduciary responsibility |
| | False claim | Intentional lie to avoid or receive restitution of funds |
| | Synthetic ID | Accounts created with stolen PII for gain (e.g., Mule accounts, loans) |
| **Unauthorized party modified payment information** | Compromised credentials | Digital access information obtained by an unauthorized party and used for gain |
| | Impersonated authorized party | Unauthorized party has stolen information that can be used to access funds |
| | Physical alteration | Tampering with a physical payment instrument |
| **Unauthorized party took over account** | Compromised credentials | Digital access information obtained by an unauthorized party and used for gain |
| | Impersonated authorized party | Unauthorized party has stolen information that can be used to access funds |
| **Unauthorized party misused account information** | Digital payment | Electronic payment is initiated with stolen account data (e.g., ACH debit, card fraud) |
| | Physical forgery/ counterfeit | Imitation physical payment instrument is used to initiate a payment (e.g., fraudulent check) |

### ScamClassifier Model Definitions

| | |
|---|---|
| **Merchandise scam** | Purchase of merchandise that is never delivered or is substantially different from the advertised description or quality (e.g., fake tickets, pet scams.) |
| **Investment scam** | An investment in a financial asset with expectation of a high return rate based on false promises (e.g., fake business opportunities, fake cryptocurrency.) |
| **Property sale or rental scam** | The purchase or rental of a home, apartment, or property that was fictitious, not available, or was not rightfully owned by the offering party. |
| **Romance impostor scam** | The use of a fictitious online identity to establish a trusted relationship (romance or friendship) with intent to request money using a false situation (e.g., travel, medical bills, emergencies.) |
| **Government impostor scam** | Scammer poses as government agency, law enforcement, or a trusted authority to deceive a party to send a payment or sensitive information often to avoid arrest, financial penalties, or reputational harm (e.g., IRS back taxes, arrest warrant issued.) |
| **Bank imposter scam** | Scammer poses as a legitimate financial institution or bank representative to deceive a party into revealing confidential banking information or sending a payment to protect the customer's money (e.g., fraud department representative.) |
| **Business imposter scam** | Scammer imitates a legitimate business, company or brand to deceive a victim into making payments or providing sensitive information (e.g., tech support, business email compromise (BEC), lottery/prizes.) |
| **Relative/family/friend scam** | Scammer poses as a family member or representative of family member to request money based on a false situation or emergency (e.g., kidnapping, arrest). |
| **Other trusted party scam** | Scammer poses as a specific role to engage another person to request money based on a false expectation (e.g., charity/disaster relief, babysitter scam.) |