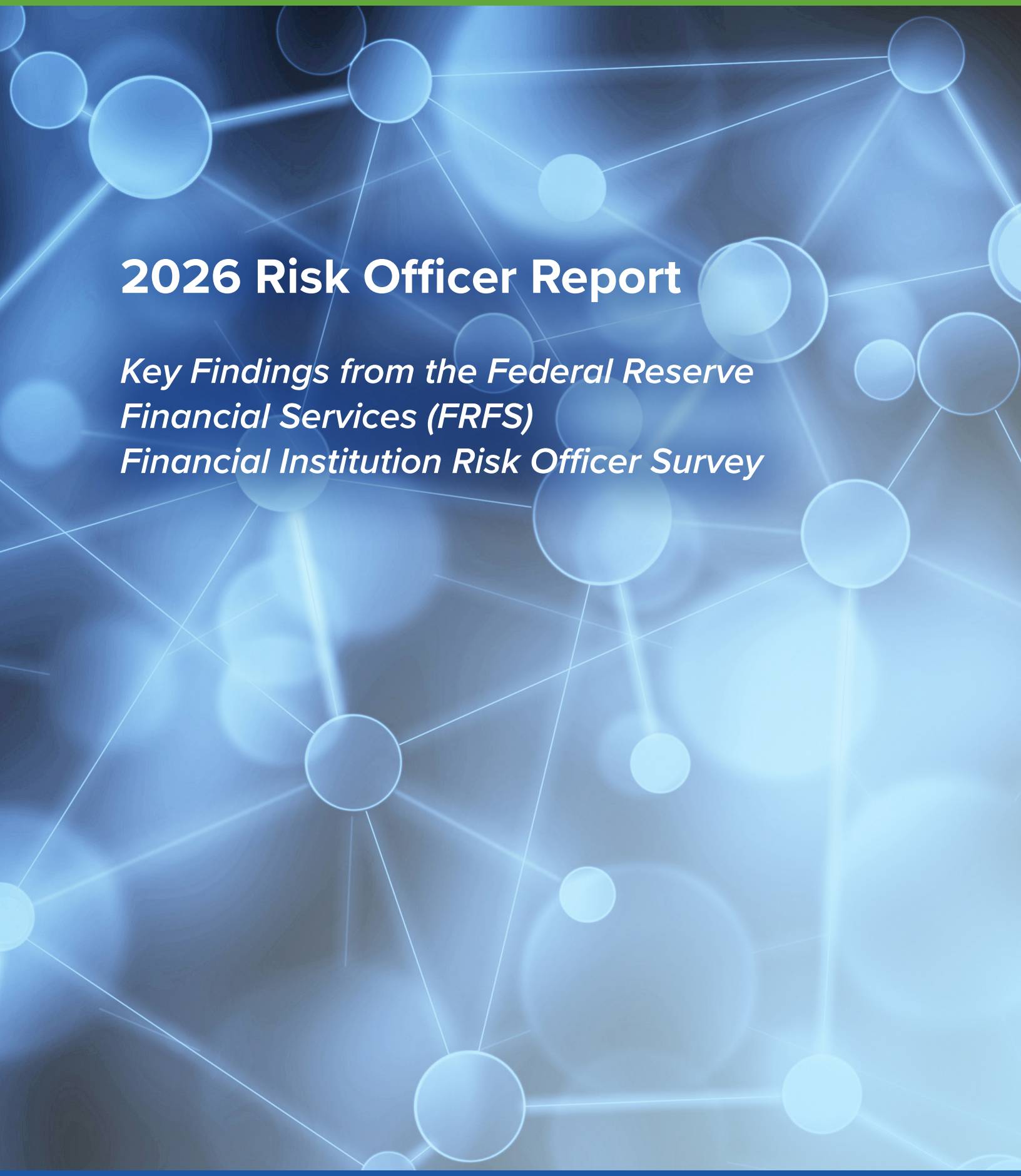


2026 Risk Officer Report

Key Findings from the Federal Reserve Financial Services (FRFS) Financial Institution Risk Officer Survey

THE FEDERAL RESERVE
Financial Services

Table of Contents

About This Survey

This annual survey was conducted by Federal Reserve Financial Services, an integrated operational structure within the Federal Reserve that is responsible for managing critical payment services, as well as collaborating with the broader industry on payment improvement initiatives. FRFS provides several tools to support institutions in supplementing their existing efforts to identify and mitigate payments risk.

Questions were submitted to senior risk experts at institutions that use financial services offered by FRFS, including cash, check, ACH, funds transfer and instant payments. Because FRFS offers these services, 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. The insights are more helpful when looking across multiple years. The sampling margin of error is +/- 6% at a 95% confidence level.

Executive Summary

The survey, conducted in the fourth quarter of 2025, collected responses about their risk experience from over 400 financial institutions of various sizes across the United States. Across all payment channels, the survey showed fraud being driven by a combination of evolving criminal tactics, increased digital exposure and rising scam activity that exploits both customers and institutions. While the specific fraud patterns differ across debit, check, wire, ACH and money mule account activity, a clear theme emerged: financial institutions are experiencing broad increases in both fraud attempts and losses, with criminals increasingly using techniques such as impersonation, social engineering and credential compromises.

Debit card fraud remained the most widespread, with nearly universal exposure to card not present and did not authorize/recognize incidents, while never received fraud showed signs of improvement. Check fraud continued its multi-year resurgence, with significant reported increases in counterfeit checks, check washing, forgery and physical alteration — patterns that align with rising losses and ongoing challenges in early detection. Wire fraud trends reinforce the threat landscape pattern, showing persistent growth in reports of account holder scams, business email compromise and money mule-driven transfers, all of which highlight the increasing sophistication of social engineering-based attacks.

ACH-related fraud reflected similar dynamics, with sharp reported increases in account holder scams, business email compromise, unauthorized debits and account takeover. Data organized based on the FraudClassifier℠ model confirmed these patterns at a broader level, showing no decline in any major fraud event category, substantial growth in impersonation and digital payment fraud, and a notable rise in account takeover activity as criminals exploit stolen or compromised credentials.

Money mule account activity tied these channel-specific trends together, as institutions reported rising levels of deception involving legitimate customers, more virtual and synthetic identity account openings, and detection processes that remain highly manual and often occur too late. In many cases, institutions first learned about a money-mule account only after funds were depleted. Collectively, the fraud channel landscape points to increasingly interconnected threats that demand more proactive, collaborative and data-driven defenses across the industry.

The survey questions are listed at the end of this document.

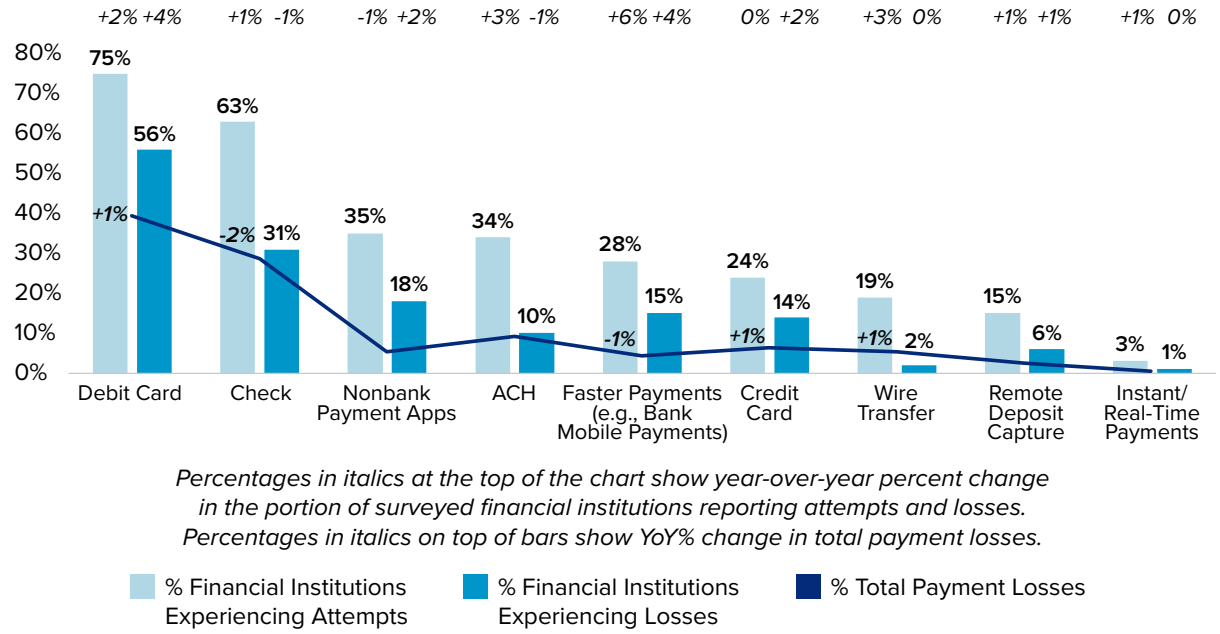
For more information about fraud and scams, contact securepayments@bos.frb.org.
For ideas, questions or to learn more about the survey, contact Robert.A.Williams@chi.frb.org.

Research

Fraud Risk Summary by Payment Type

Surveyed financial institutions most frequently reported experiencing fraud attempts and losses related to debit cards and checks. Faster payments (e.g., bank mobile payments) are a growing area of concern, as this payment category had the largest increase in attempted fraud and losses compared to the previous year. At the same time, the share that each payment type contributes to overall fraud losses has stayed largely stable over the past three years of surveys, with only minor increases or decreases in individual payment types.

Chart 1: Fraud Risk Summary by Payment Type



Percentages in italics at the top of the chart show year-over-year percent change in the portion of surveyed financial institutions reporting attempts and losses. Percentages in italics on top of bars show YoY% change in total payment losses.

% Financial Institutions Experiencing Attempts
% Financial Institutions Experiencing Losses
% Total Payment Losses

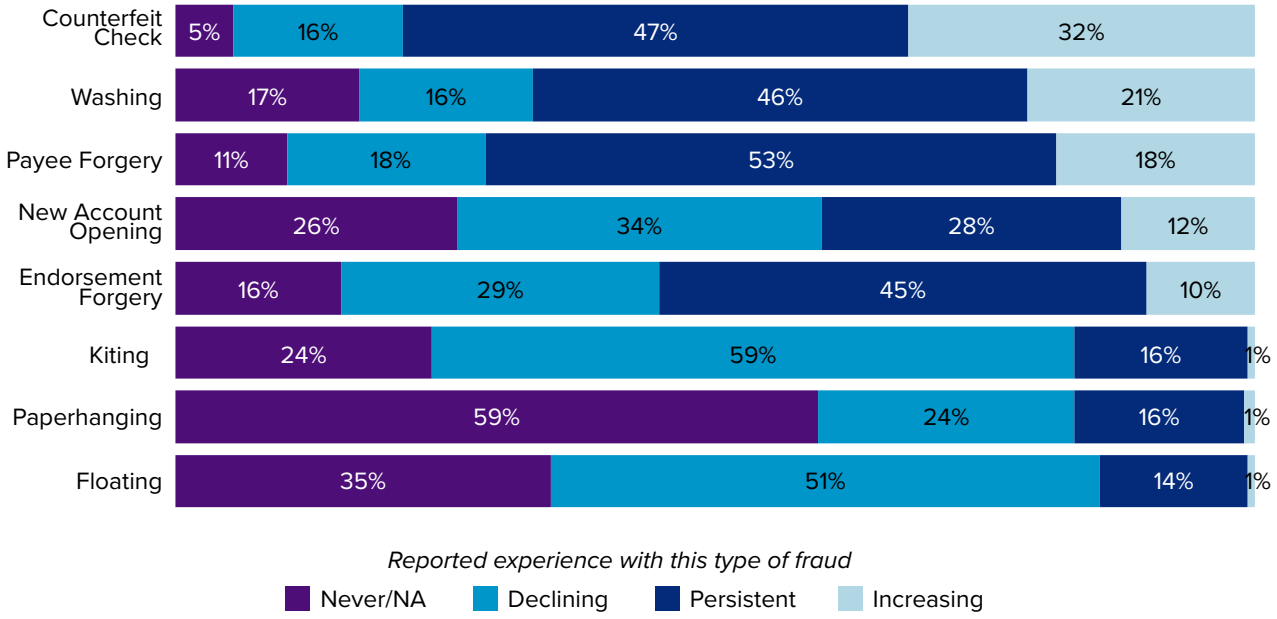
- Debit card payments continued to be the most targeted channel, with 75% of surveyed financial institutions experiencing attempts. Compared to the previous year, 4% more financial institutions had losses from this type of fraud, and survey respondents estimated that it accounted for 40% of their total losses from payments fraud.
- Check fraud remained the second most-frequently reported type of fraud. A total of 63% of surveyed financial institutions reported experiencing check fraud attempts and 31% of those divulged they had losses from it, though the portion of losses from this type of fraud decreased by 2% compared to the previous year.

- Fraud attempts related to faster payments increased by 6%, reported financial institutions, and the number reporting losses increased by 4% compared to last year. Estimated losses from faster payments fraud decreased by 1%.
- Instant/real-time payments remained a relative bright spot, with relatively few reported fraud attempts and losses.
- As estimated by surveyed institutions, the share of fraud loss expense related to each payment type has been broadly stable for three years, with 1% increases in each of debit, credit and wire payments compared to last year.

Specific Fraud Events

Financial institutions reported that many different types of check fraud are increasing as criminals exploit stolen checks and new accounts. Reports of debit card fraud remained elevated. While financial institutions reported increases in many types of fraud, some categories showed signs of improvement.

Chart 2a: Specific Check Fraud Events



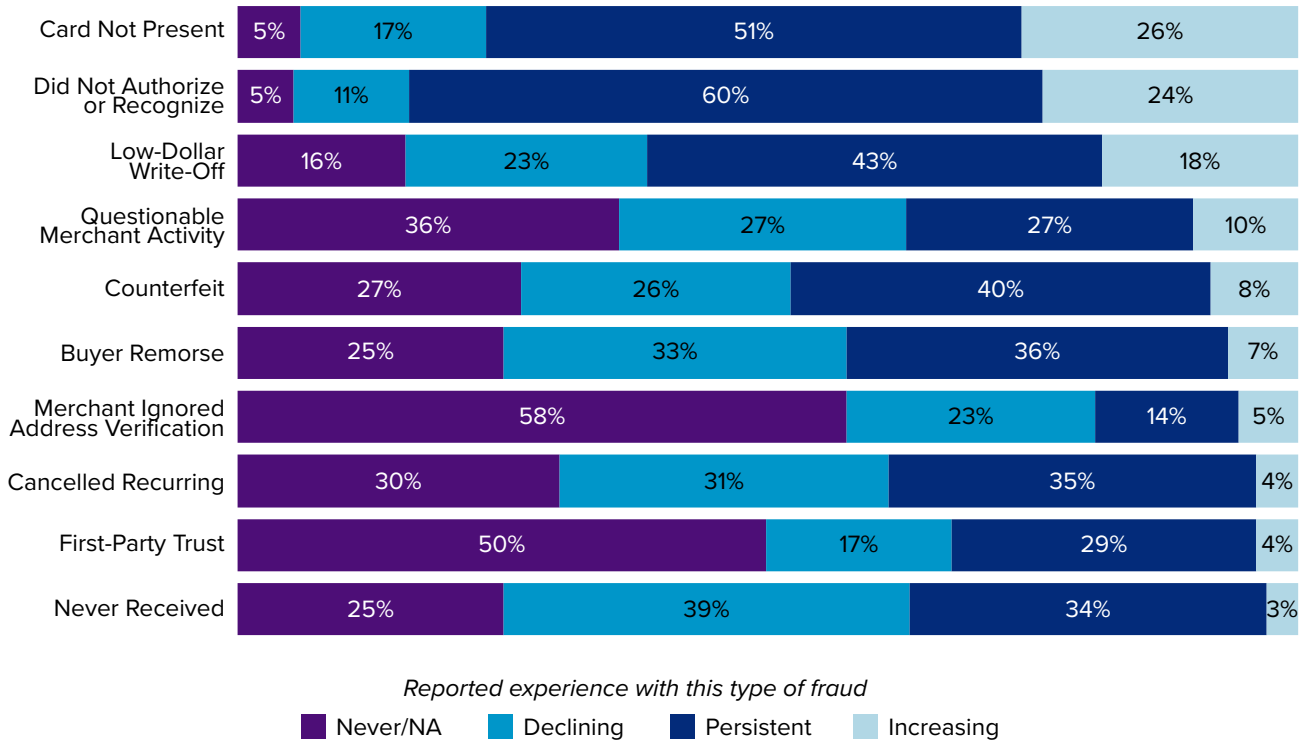
Check

- Traditional check fraud was on the rise, with 32% of financial institutions reporting increases in counterfeiting, 21% reporting increases in check washing, and 18% reporting increases in payee forgery.
- New account openings showed heightened vulnerability, as 3% more financial institutions reported that this type of fraud was persistent or increasing compared to last year.
- Stolen checks dominated results, with 89% of respondents reported that they experienced payee forgery, 84% disclosed endorsement forgery and 83% reported check washing.

Respondent-Identified Solutions to Mitigate Check Fraud Losses

- AI image analysis to detect alterations and anomalies
- Positive Pay to stop unauthorized checks from clearing
- Manual reviews and staff training to catch fraud
- Advance monitoring for new account transactions

Chart 2b: Specific Debit Card Fraud Events



Debit Cards

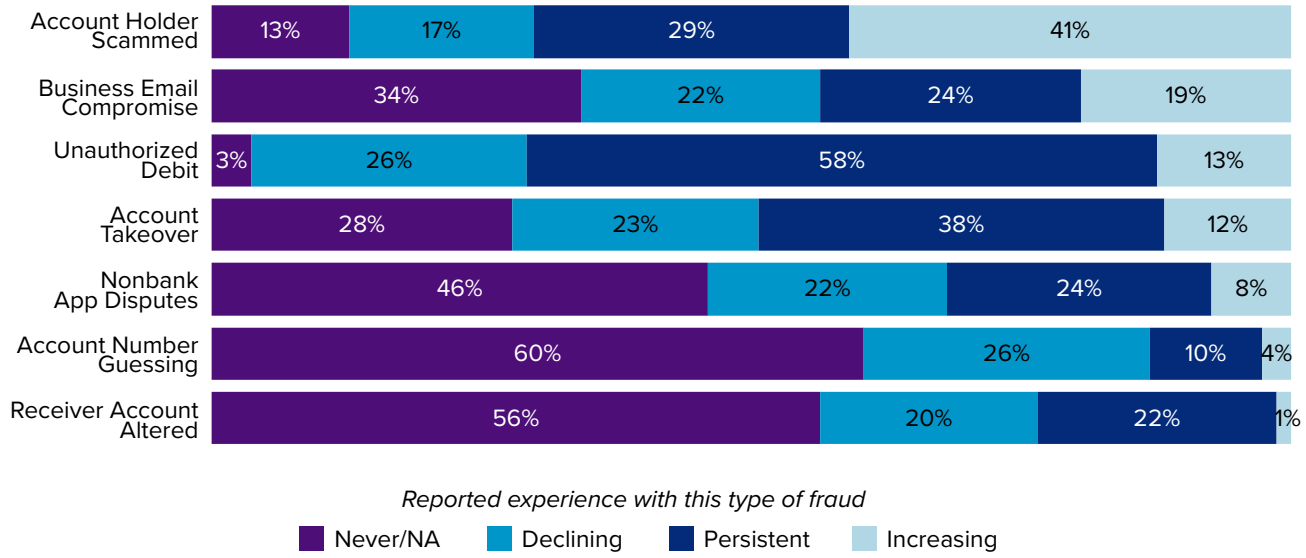
- Card not present fraud was nearly universal, with 94% of financial institutions reporting that they experienced it and 26% reported that it is increasing.
- Did not authorize/recognize cases were similarly common, with 95% of financial institutions experiencing them, 24% reported increases and 60% described this type of fraud as persistent.
- Never received fraud showed some positive results, as 39% of institutions reported that it is declining.

Respondent-Identified Solutions to Mitigate Debit Card Fraud Losses

- Real-time monitoring alerts with self-service controls
- Network analytics detection and baseline fraud protection
- 3D Secure and CVV rules to prevent card not present fraud
- Dark web scanning
- Proactive debit card replacement

Financial institutions reported increases in some types of ACH fraud, noting exposure to social engineering and email compromise. Out of all respondents who experienced losses from ACH fraud, nearly all (97%) reported unauthorized debits. Wire fraud levels remained elevated, with broad exposure to scams, compromise activity, mule operations and account takeover significantly contributing to industry risk.

Chart 2c: Specific ACH Fraud Events



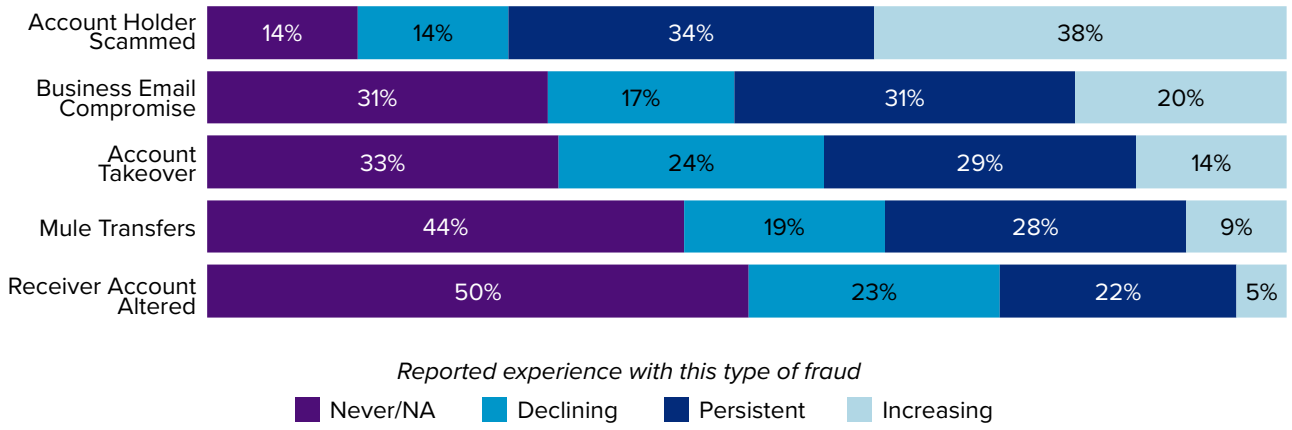
ACH

- Account holder scam activity showed the strongest upward trend, as 41% of respondents reported that it is increasing.
- Business email compromise reflected similar growth, as 19% of financial institutions reported that it is increasing.
- Unauthorized debit fraud was widespread, with 97% of financial institutions reporting that they experienced it in the past year, though only 13% noted that it was increasing.
- A total of 12% of financial institutions reported that account takeover fraud was increasing.

Respondent-Identified Solutions to Mitigate ACH Fraud Losses

- ACH Positive Pay with name verification controls
- Real-time behavioral analytics to detect account takeover
- AI and machine learning to identify transaction anomalies
- Manual review remains critical despite automation

Chart 2d: Specific Wire Fraud Events



Wire

- A total of 38% of surveyed financial institutions reported that account holder scams are increasing and 20% reported increases in business email compromise
- Account takeover fraud remained a significant threat for a portion of financial institutions, as 14% reported increases.
- Mule transfers affected more than half of institutions, and 9% reported increasing exposure, underscoring the ongoing scale of this fraud avenue.

Respondent-Identified Solutions to Mitigate Wire Fraud Losses

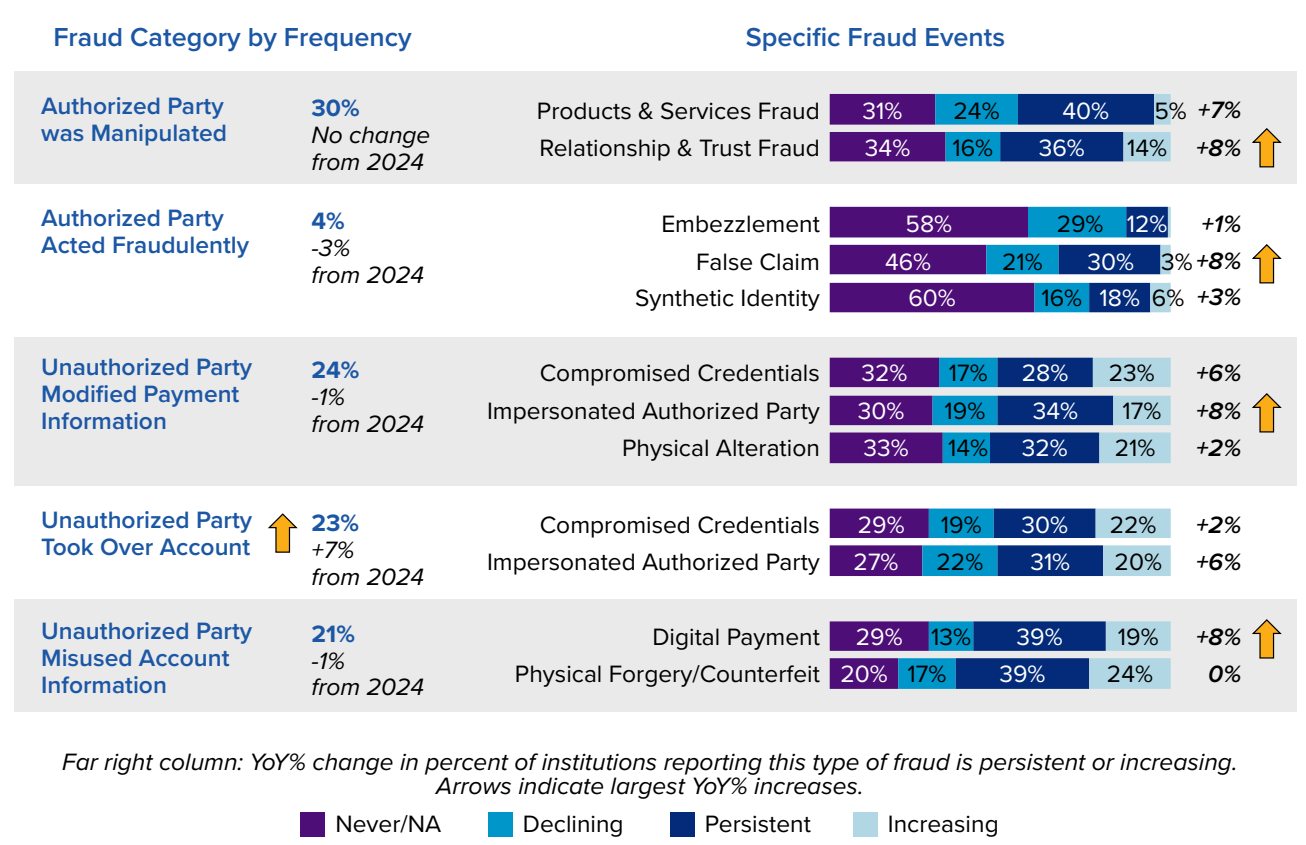
- Callbacks and PIN authorization codes mandatory
- Biometric identity verification in platforms
- Real-time behavioral monitoring alerts for anomalies
- Education on business email compromise to help prevent social engineering attacks

FraudClassifier℠ Model Events

Surveyed institutions sometimes categorized types of fraud in their responses based on the FraudClassifier model, which is not a fraud detection tool but rather a classification structure that can help users consistently identify how the fraud occurred. Furthermore, the model can help users uncover statistics on what facilitated fraud incidents, such as compromised credentials, impersonation of authorized parties, or relationship and trust scams.

Survey responses indicate that while most high-level fraud categories remained stable, financial institutions are seeing a meaningful shift toward greater account takeover activity as unauthorized-party fraud rises. At the same time, increased numbers of financial institutions reported experiencing many types of these fraud events, which demonstrates the expanding complexity of threats facing financial institutions.

Chart 3a and 3b: FraudClassifier Experience



- Account takeover fraud is emerging as a growing risk, reflected in a 7% increase in financial institutions reporting that an unauthorized party took over the account and a 3% decline in instances of an authorized party acting fraudulently.
- Across specific fraud events, no surveyed financial institutions reported declines in any categories of fraud as defined by the FraudClassifier model. The largest increases in reported fraud events included relationship and trust fraud (+8%), false claim (+8%), impersonated authorized party (+8%) and digital payment fraud (+8%).
- Indicators of intensifying check-related and credential-driven fraud persisted, with 23% of financial institutions reporting increased compromised credentials, 24% reporting rising physical forgery/counterfeit, and others reporting growing concerns about physical alteration and other check fraud-aligned behaviors.

Illustrative Challenges Reported by Survey Respondents

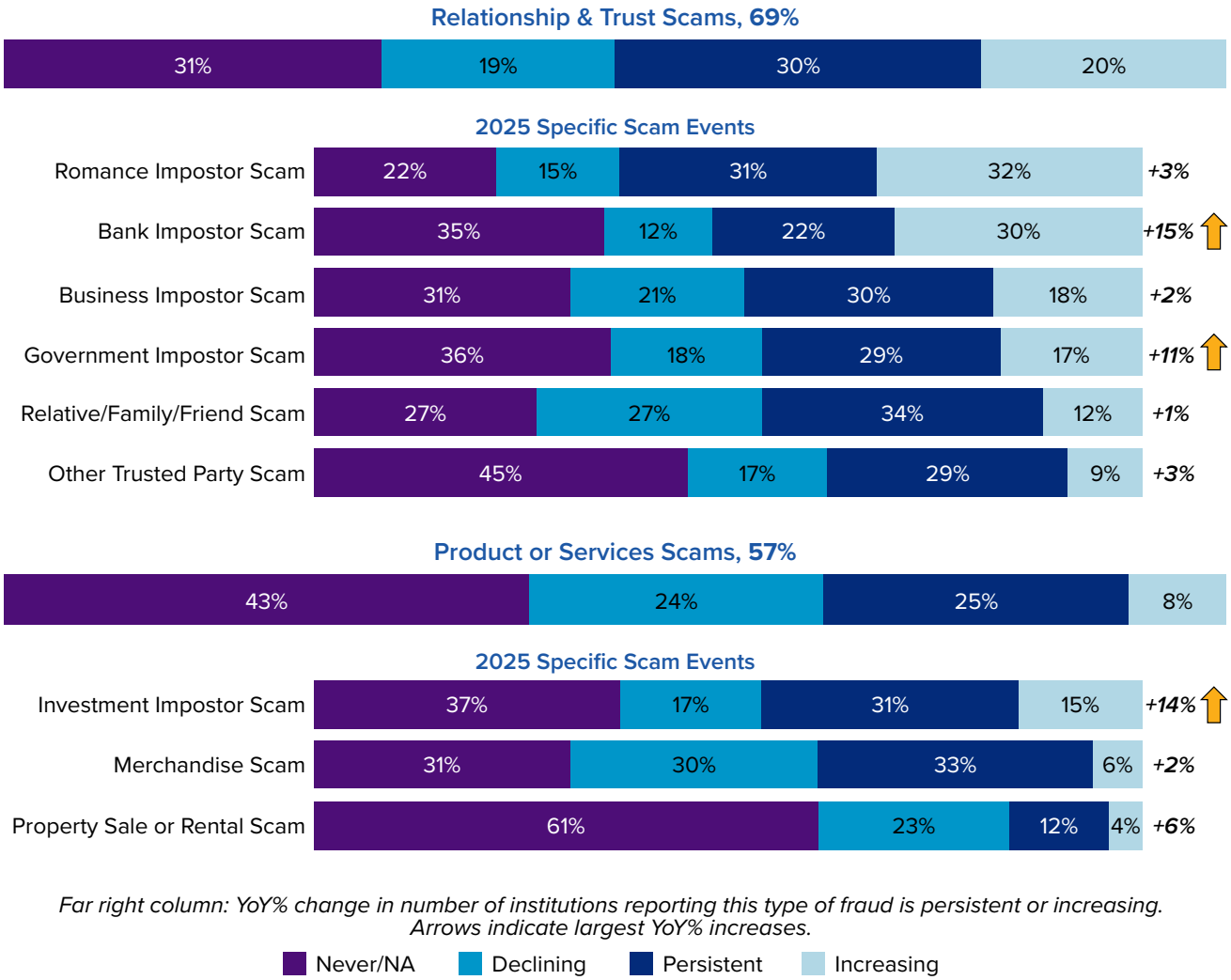
"Balancing system limitations, mitigation tools and member experience. The more secure you make your systems, the more inconvenience it places on the account holders."
Large Credit Union

ScamClassifier℠ Model Events

Like the FraudClassifier model, the ScamClassifier model is not used to detect scams, but instead as a classification structure that can help users consistently identify how the scams occurred and what factors facilitated the scams. When used together, the models can help organizations to improve mitigation strategies and internal training through identification of fraud and scam types, enhanced reporting, and customer education on specific trends.

Survey results on scams categorized using the ScamClassifier model showed that scam activity remains widespread. Financial institutions most frequently reported relationship and trust-based scams. Additionally, compared to last year, more financial institutions indicated that they are seeing increasing amounts of impersonation-driven and investment-related scams.

Chart 4: ScamClassifier Experience



Far right column: YoY% change in number of institutions reporting this type of fraud is persistent or increasing. Arrows indicate largest YoY% increases.

Never/NA Declining Persistent Increasing

- Relationship and trust scams remained the dominant category, experienced by 69% of financial institutions, with 20% reporting that these types of scams are increasing.
- The fastest-growing scam types included bank impostor scams, with a 15% increase in the number of financial institutions reporting that this type of scam is persistent or increasing compared to last year. Additionally, the number of financial institutions who reported that investment scams are persistent or increasing went up by 14%, and the number who said government impostor scams were increasing or persistent rose by 11%.
- 32% of financial institutions reported that romance impostor scams were increasing, 30% said bank impostor scams were increasing and 18% said business impostor scams were rising.

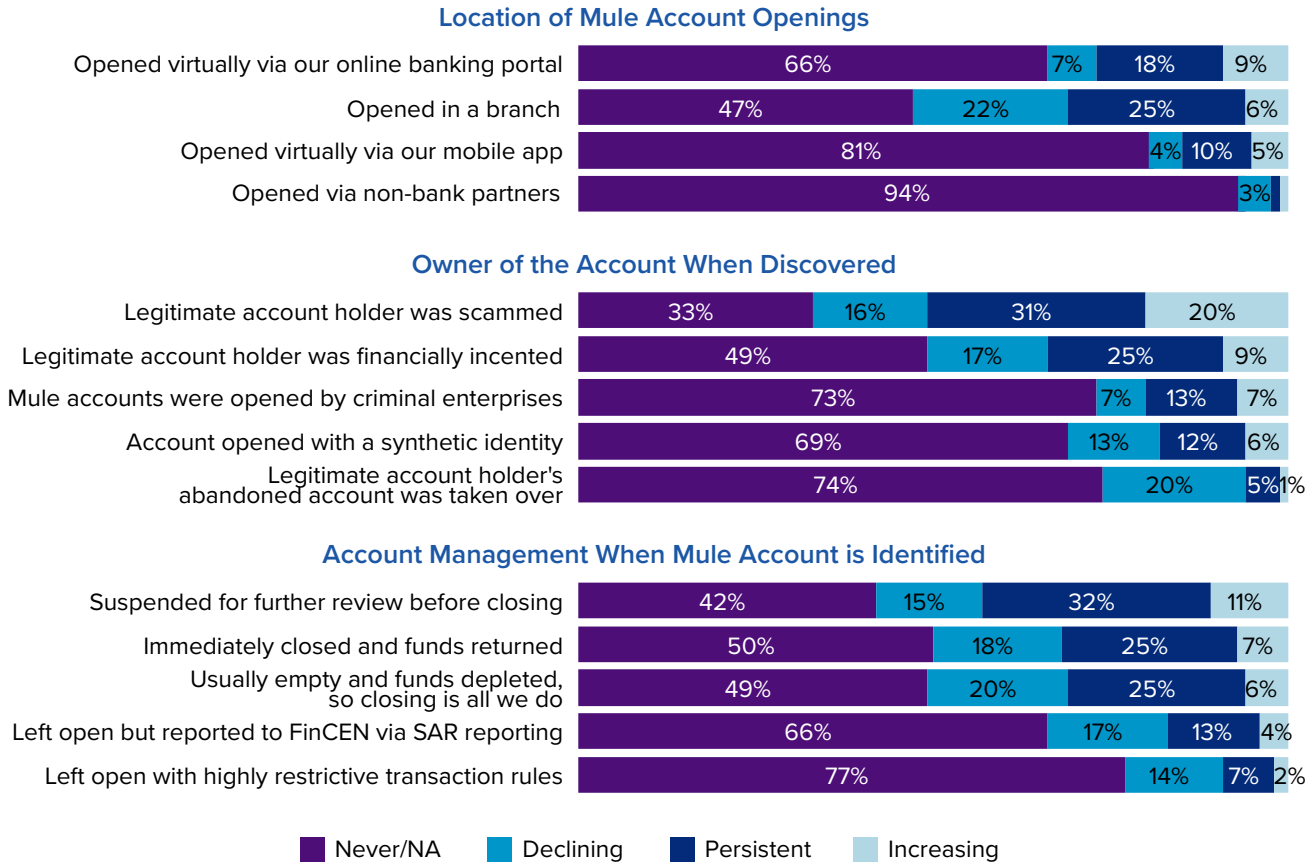
Illustrative Challenges Reported by Survey Respondents

"Keeping our employees aware of current trends and red flags of fraud. As scams are always evolving and changing, training our staff what to watch for becomes more difficult." *Regional Commercial Bank*

Mule Accounts

Mule account activity continued to challenge financial institutions across the full payments lifecycle, from account opening to detection to eventual closure, reflecting both human-driven and criminal-enterprise threats. These patterns highlighted growing operational strain as institutions continued to rely heavily on manual processes and often identified mule activity only after losses or external alerts.

Chart 5: Mule Accounts



- According to this survey, mule accounts are most often opened in branches. A total of 53% of surveyed financial institutions reported experiencing this type of fraud, with growth in virtual openings. Two-thirds of mule account fraud involves legitimate customers who are deceived, while synthetic identity and criminal-enterprise openings are steadily increasing.
- Discovery of mule account fraud frequently occurs too late. A total of 51% of institutions surveyed reported that they identified mule activity only after losses, underscoring the reactive nature of current detection practices.
- Account closure actions vary widely, with 58% suspending accounts for review and 34% leaving accounts open but filing suspicious activity reports (SARs). Many institutions reported that funds were already depleted by the time the mule account was confirmed.

Illustrative Challenges Reported by Survey Respondents

"[A common issue with] ACH [is that we are] unable to contact the receiving depository financial institution [RDFI] or originating depository financial institution [ODFI] in [a] timely manner to [address potential] fraud payments — sometimes [our] request for contact goes unanswered. For wire transfers, [it is being] unable to contact [the] RDFI in [a] timely manner." *Large Community Bank*

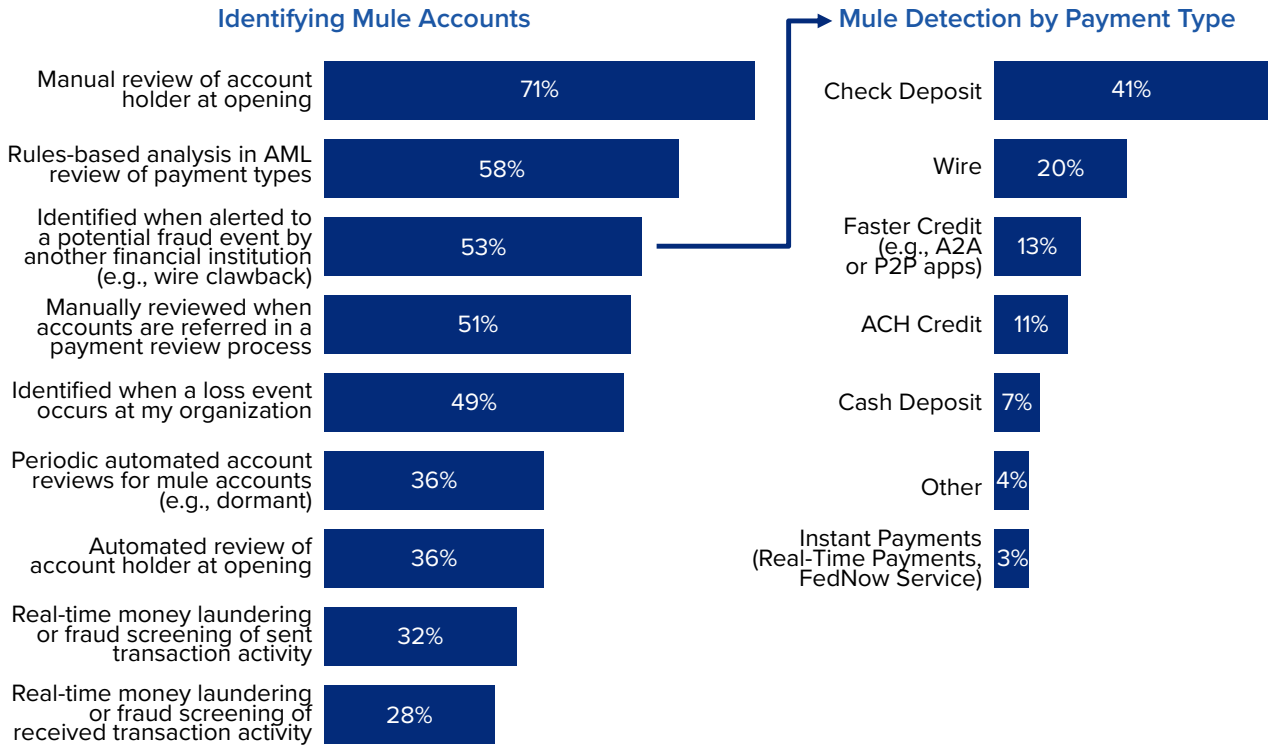
"Keeping our employees aware of current trends and red flags of fraud. As scams are always evolving and changing, training our staff what to watch for becomes more difficult." *Regional Commercial Bank*

"Limited system integration and data visibility create delays in detecting anomalies, while resource constraints and manual workarounds increase residual risk. Strengthening automation, cross-platform alerts and capacity alignment is essential to close these gaps." *Regional Commercial Bank*

Finding Mule Accounts and Anti-Money Laundering (AML)

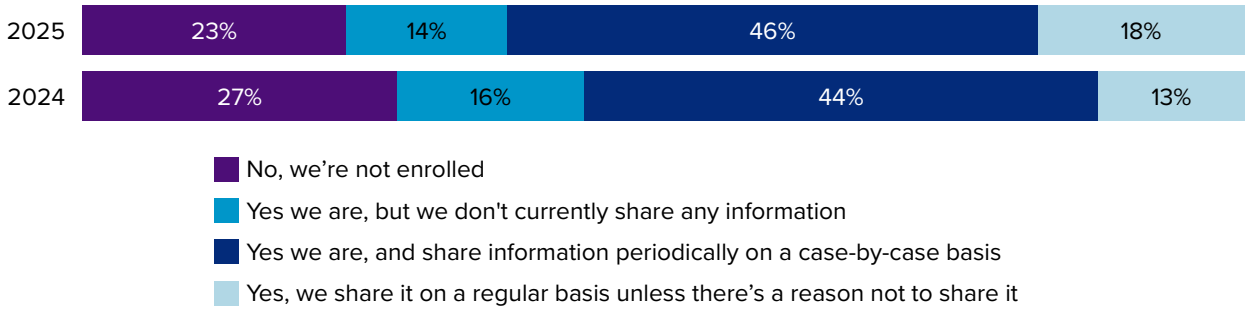
Mule account detection is still largely manual, resulting in many institutions learning of activity only after losses or external alerts. According to surveyed financial institutions, the most common triggers for identifying a mule account come from check-related fraud (41%) or wire transfer clawbacks (20%), underscoring how often discovery occurs only once transactional harm is already underway.

Chart 6a and 6b: Finding Mule Accounts and AML



- Detection remains heavily manual, with 71% of institutions relying on manual review and less than half using automation, which can lead to delayed identification — 53% of respondents report learning of mule activity from another financial institution, and 49% only discover it after losses occur.
- When alerted to a potential mule account by another financial institution, 41% of respndents reported that the most frequent catalyst is check payments. Mules will often deposit fraudulent checks or originate wire transfers and then try to claw those payments back.

Chart 6c: Participation in and Utilization of FinCEN

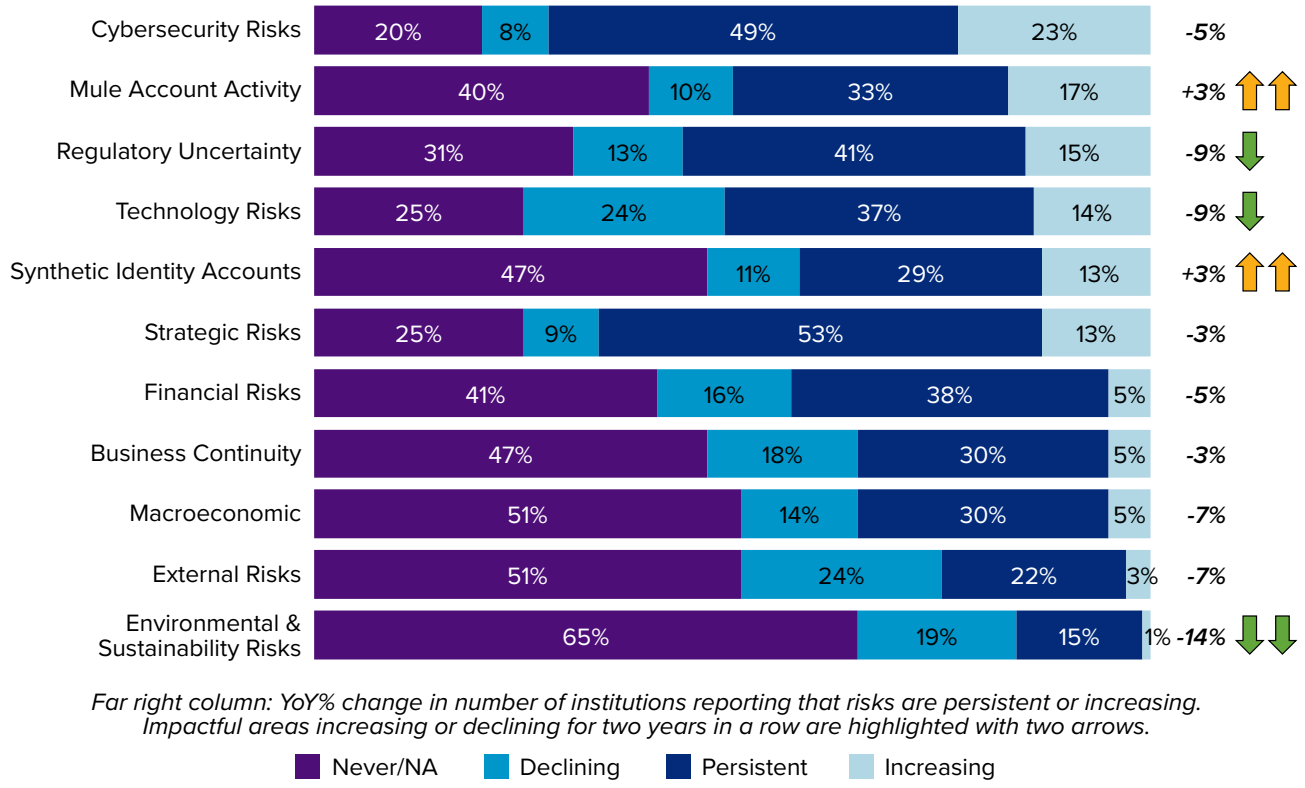


Despite modest enrollment gains, information sharing under FinCEN 314(b) remains constrained, with about a quarter of institutions still unenrolled and fewer than one in five sharing activity regularly, even as participation and use show gradual improvement.

Impactful Areas on Risk Profiles

Risk professionals at financial institutions reported that several risk categories continue to exert meaningful influence on their risk profiles, though with shifting momentum. Cybersecurity, strategic risk and scam-related risks remained highly impactful for financial institutions, while other risk categories show notable declines in perceived impact, including environmental and sustainability, regulatory uncertainty and technology. Impactful areas increasing or declining for two years in a row are highlighted with two arrows.

Chart 7: 2025 Impactful Areas on Risk Profiles



Far right column: YoY% change in number of institutions reporting that risks are persistent or increasing. Impactful areas increasing or declining for two years in a row are highlighted with two arrows.

Areas Remaining Highly Impactful

- Cybersecurity remains a critical risk, as 72% of financial institutions indicated that it is persistent or increasing.
- Strategic risk also stayed elevated, with two thirds citing that it is persistent or increasing.
- There was a 3% increase in the number of financial institutions rating risks from mule accounts and synthetic ID accounts as impactful and persistent or increasing, trending up two years in a row.

Areas Showing Declines in Impact

Several risk categories showed meaningful reductions in the number of financial institutions rating them as impactful and persistent, or impactful and increasing, including environmental and sustainability (a 14% decrease), regulatory uncertainty (9% decrease) and technology (9% decrease).

Illustrative Challenges Reported by Survey Respondents

"Cyber is believed to be an increasing risk and we are devoting more time and resources to that area. It is difficult to keep pace with the knowledge and execution of the criminal element." *Large Community Bank*

"Disjointed systems — systems that don't connect to each other and create duplicative work that takes our focus away from current issues." *Regional Credit Union*

"Uncertainty about regulations for banks, fintechs and other nonbank service providers. Cryptocurrency, stablecoin and central bank digital currencies are all threats to the conventional banking system." *Regional Commercial Bank*

FRFS Resources

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 by 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
- Check Fraud Mitigation Toolkit
- Account Takeover Fraud Toolkit

Other References

Industry Resources

1. Suspicious Activity Report (SAR) Statistics from the Financial Crimes Enforcement Network (FinCEN.gov)
2. Financial Trend Analyses from the Financial Crimes Enforcement Network (FinCEN.gov)
3. Fraud Reports from the Federal Trade Commission Consumer Sentinel Network (tableau.com)
4. Avoiding and Reporting Scams from the Federal Trade Commission (consumer.FTC.gov)
5. Federal Bureau of Investigation Bank Crime Statistics (FBI.gov)
6. U.S. Department of the Treasury 2026 National Money Laundering Risk Assessment (PDF, Treasury.gov)
7. Fraud and Scams Info from the Consumer Financial Protection Bureau (consumerfinance.gov)
8. Fraud Resources from the Office of the Comptroller of the Currency (occ.treas.gov)
9. Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) InfoBase (bsaaml.ffiec.gov)
10. Fraud Resources from the American Bankers Association (ABA®) (aba.com)
11. Payments Fraud Info from SWIFT® (SWIFT.com)

Other Industry Analysis

1. Navigating Cyber 2025: Annual Threat Review and Predictions from the Financial Services Information Sharing and Analysis Center (FS-ISAC) (fsisac.com)
2. Forecasting the Rise of Push Payment Scams — The Fraud Consumers Are Tricked Into Authorizing (Deloitte.com)
3. How Payments Fraud is Growing in Scale and Sophistication and What Companies Can Do to Fight Back (Mastercard.com)
4. Bank Policy Institute (BPI) Fraud and Scam Prevention Playbook (BPI.com)
5. The Impact of Fraud on Financial Institutions (Somos.com)
6. Fighting Payments Fraud from Stolen Checks to “Deepfake” Scams (RichmondFed.gov)
7. Financial Fraud Through the Lens of Extended Fraud Alerts (PDF, PhiladelphiaFed.org)
8. Using Digital Identity to Support Access to Payments (PDF, AtlantaFed.org)
9. Global Scams on the Rise: Over Half of Adults Report Scam Encounters (GASA.org)
10. Global Anti-Financial Crime (AFC) Threats Report 2025 (ACAMS.org)

Respondent Profile (403 Responses)

Bank	75%
Credit Union	25%
Other	<1%

Assets Over $10 Billion	12%
Assets $1 Billion - $10 Billion	29%
Assets $100M - $1 Billion	45%
Assets Under $100M	13%
Foreign Banks, Other	1%

Detailed Questions and Available Selections

Chart 1: Fraud Risk Summary by Payment Type

Survey question: For each of the following payment methods, how often have your organization and account holders (been subjected to attempted fraud/experienced actual losses from fraud) in the past 12 months?

Available selections:
- Never
- Rarely
- Sometimes
- Frequently
- Do not know or not applicable

Survey question: On estimate, what portion of your institution's payment fraud loss expenses have occurred with these payment methods in the past 12 months?

Chart 2a: Specific Fraud Events

Survey question: Which best describes your institution's experience with the type of check fraud you experienced in the past 12 months?

Available selections:
- Do not know or not applicable
- Never
- Experienced but declining
- Experienced and persistent
- Experienced and increasing

Chart 2b: Specific Fraud Events

Survey question: Which best describes your institution's experience with the type of debit fraud you experienced in the past 12 months?

Available selections:
- Do not know or not applicable
- Never
- Experienced but declining
- Experienced and persistent
- Experienced and increasing

Chart 2c: Specific Fraud Events

Survey question: Which best describes your institution's experience with the type of ACH fraud you experienced in the past 12 months?

Available selections:
- Do not know or not applicable
- Never
- Experienced but declining
- Experienced and persistent
- Experienced and increasing

Chart 2d: Specific Fraud Events

Survey question: Which best describes your institution's experience with the type of wire fraud you experienced in the past 12 months?

Available selections:
- Do not know or not applicable
- Never
- Experienced but declining
- Experienced and persistent
- Experienced and increasing

Chart 3a: FraudClassifier Model Events

Survey question: Please rank the following five types of payment fraud by frequency of occurrence in your institution over the past 12 months.

Chart 3b: FraudClassifier Model Events

Survey question: 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 4: ScamClassifier Model Events

Survey question: 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

Chart 5: Mule Accounts

Survey question: How often have you seen the following sources of mule accounts in your or your peer organizations in your markets during the past 12 months?

Available selections:
- Do not know or not applicable
- Never
- Experienced but declining
- Experienced and persistent
- Experienced and increasing

Chart 6a: Finding Mule Accounts and Anti-Money Laundering (AML)

Survey question: What is your institution doing to identify accounts that may be mule accounts? Select all that apply.

Available selections:
- Manual review of account holder at opening
- Automated review of account holder at opening
- Periodic automated account reviews for mule accounts (e.g., dormant)
- Rules-based analysis in AML review of payment types
- Manually reviewed when accounts are referred in a payment review process
- Identified when a loss event occurs at my organization
- Identified when alerted to a potential fraud event by another depository institution (e.g., wire clawback)
- Real-time money laundering or fraud screening of sent transaction activity
- Real-time money laundering or fraud screening of received transaction activity

Chart 6b: Finding Mule Accounts and Anti-Money Laundering (AML)

Survey question: When alerted to a potential fraud event by another financial institution, what payment type is most often the catalyst to finding the mule account?

Available selections:
- Wire
- ACH credit
- Instant payments
- Faster credit (account-to-account (A2A) or person-to-person (P2P)) apps
- Check deposit
- Cash deposit
- Other (please specify)

Chart 6c: Finding Mule Accounts and Anti-Money Laundering (AML)

Survey question: Is your institution enrolled under FinCEN 314(b) and are you sharing fraudulent activity under it?

Available selections:
- No, we're not enrolled
- Yes we are, but we don't currently share any information
- Yes we are, and share information periodically on a case-by-case basis
- Yes, we share it on a regular basis unless there's a reason not to share it

Chart 7: Impactful Areas on Risk Profiles

Survey question: How would you rate the following trends in terms of current impact to your institution's payment risk profile?

Available selections:
- Do not know or not applicable
- No impact
- Impactful but declining
- Impactful and persistent
- Impactful and increasing

Definitions

Check Fraud Types (Chart 2a)

Term	Definition
Paperhanging	Intentionally writing bad checks
Kiting	Timing check deposits to get the cash before it bounces
Floating	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
Check washing	Chemically altering the check
Counterfeit check	Printing checks using stolen data

Debit Card Fraud Types (Chart 2b)

Term	Definition
Counterfeit	Fake cards created from stolen card data
Card not present	Transaction wasn't validated with physical card
Buyer remorse	Product or service did not perform as expected
Low-dollar write-off	Small dispute less than cost for financial institution to research
First-party trust	Authorized card holder misrepresents their use or known use of the card
Cancelled recurring	Recurring transaction charged despite revoking the permission
Did not authorize or recognize	Charge not recognized by card holder
Never received	Cardholder never received product or service
Merchant ignored address verification	Merchant failed to validate card holder address information
Questionable merchant activity	Merchant transaction was not consistent with defined type of business

ACH Fraud Types (Chart 2c)

Term	Definition
Unauthorized debit	The customer did not authorize the debit to their account
Account number guessing	Micro deposits not initiated by account holder or numerous transactions to invalid account numbers
Account takeover	Unauthorized user gains access to online banking user interface and originated transactions
Receiver account altered	Credit push transactions are altered credits redirected from intended recipient to the criminal's account
Business email compromise	The authorized credit transaction was misdirected to a criminal because the sender was deceived
Account holder scammed	Account holder was deceived through product, investment, romance scam or other scam
Nonbank app disputes	Customer disputes deposit or debit originated from a digital wallet or nonbank payment application

Wire Fraud Types (Chart 2d)

Term	Definition
Business email compromise	The authorized credit transaction was misdirected to the criminal because the sender was deceived
Money mule transfers	Received or sent transaction was later determined to be associated with networks of money mules — people who transfer illegally acquired money on behalf of someone else
Account takeover	Unauthorized user gained access to online banking user interface and originated transactions
Receiver account altered	Credit push transactions are altered credits redirected from intended recipient to the criminal's account
Account holder scammed	Account holder was deceived through product, investment, romance scam or other scam

FraudClassifier Model Definitions (Chart 3)

Term	Event	Definition
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 impostor 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 personally identifiable information (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 fraud, debit card fraud)
	Physical forgery/ counterfeit	Imitation physical payment instrument is used to initiate a payment (e.g., fraudulent check)

ScamClassifier Model Definitions (Chart 4)

Term	Definition
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 under threat of arrest, financial penalties, or reputational harm (e.g., IRS back taxes, arrest warrant issued)
Bank impostor 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., impersonating a fraud department representative)
Business impostor 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, advance payment/lottery scams)
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)