

Key Findings From the Annual Federal Reserve Financial Services (FRFS) Financial Institution Risk Officer Survey (2024)

Table of contents

About this survey Page 3

Executive summary Page 3

Research (Charts 1-6)..... Page 4

Resources Page 10

Other references Page 11

Respondent profile..... Page 13

Detailed questions and available selections Page 13

Definitions Page 14

About this survey

This annual survey was conducted by Federal Reserve Financial Services (FRFS), a collaboration of the 12 Federal Reserve Banks, and went to senior risk experts at institutions using financial services offered by FRFS. FRFS provides payment services such as 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 at an industry level and at the level of their organizations and should not rely 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 a number of tools to support institutions in supplementing their internal tools to further help identify and/or mitigate payments risk.

Executive summary

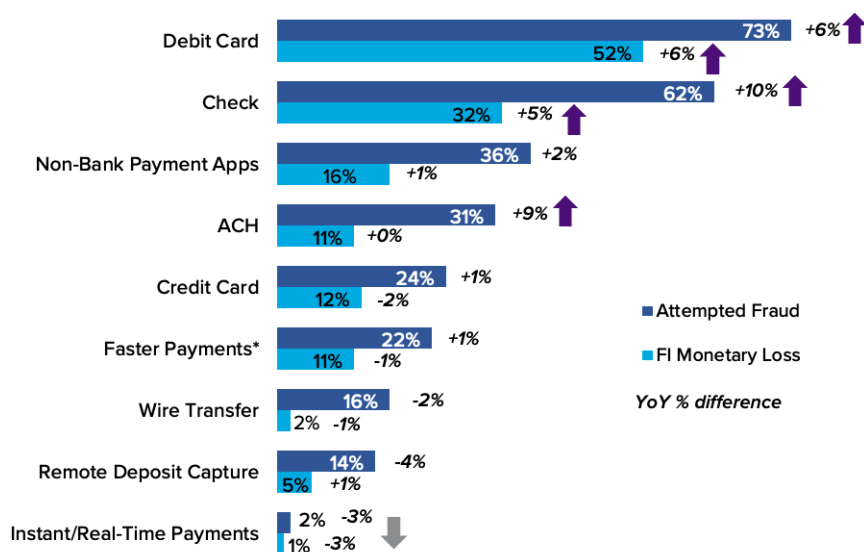
The 2024 survey collected responses from over 360 financial institutions (FIs) of various sizes across the United States. This summary will focus on fraud and its associated losses. Industry experience with fraud is compared by payment system and further explained with respondents' view of a directional expectation of trend. The summary concludes with FIs' perception of risks impacting their risk profile. **See footnotes for detailed questions*

Research

CHART 1

The top payment types for attempted fraud and losses were debit, check, non-bank payment apps and ACH.

Most Frequently Experienced Fraud and Losses by Payment Type



*e.g., mobile payments

- Number of FIs experiencing fraud attempts grew significantly in check (+10%), ACH (+9%) and debit card (+6%).
- ACH fraud attempts surpassed credit card fraud attempts compared to 2023 levels while losses experienced held steady.
- Number of FIs with monetary losses increased in check (+5%) and debit card (+6%).
- Instant/real-time payments fraud attempts and losses decreased (-3%) in 2024.

Illustrative Challenges

“Customers are careless with their banking information and share it when they should not.” (\$100M-\$1B)

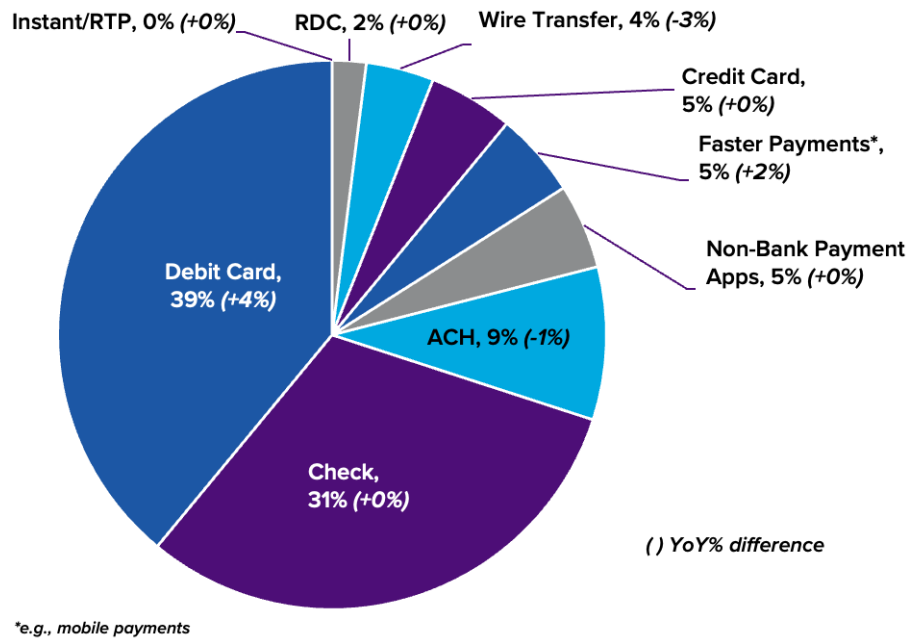
“The most effective mitigation tools are perceived to detract from a positive customer experience.” (\$1B+)

“Disparate systems needing to work together and not be so siloed, further integration required.” (\$1B+)

CHART 2

Debit card loss expenses increased (+4%), consistent with the rise of debit card fraud attempts and monetary losses described above. The share of losses by FI did not significantly change from 2023.

Fraud Loss Expense by Payment Type

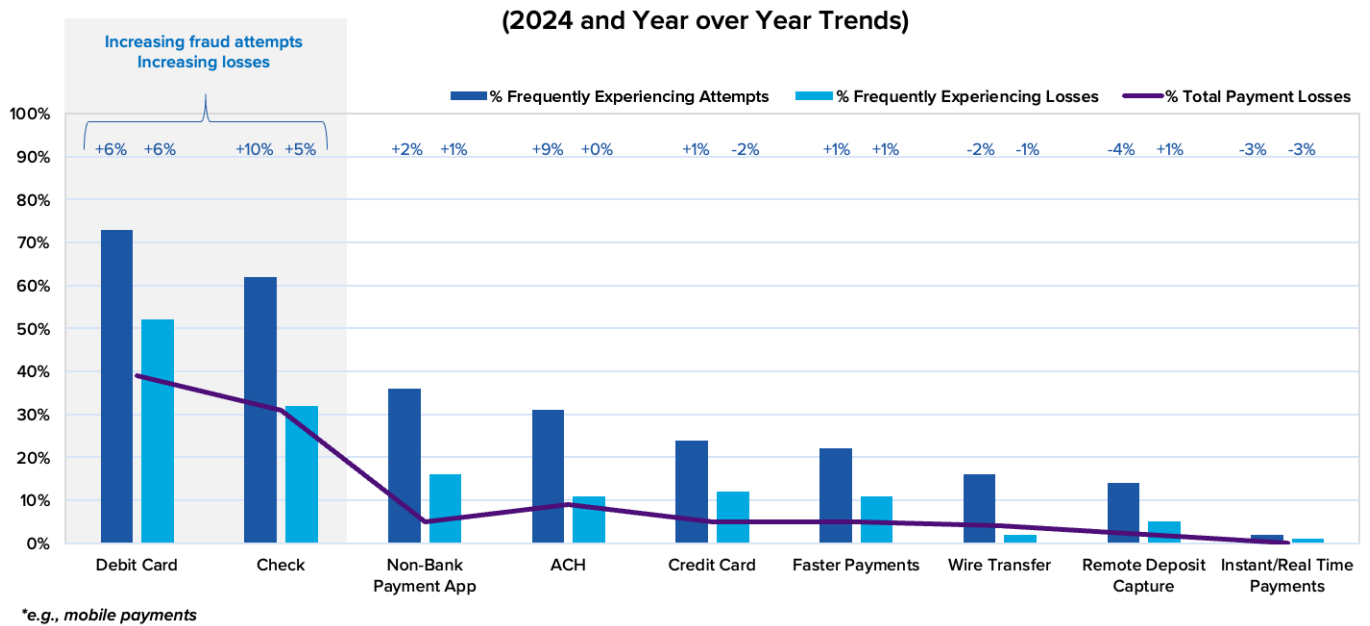


- Check average loss expenses remained near debit card levels.
- ACH (-1%) and wire transfer (-3%) loss expense declined, while faster payments (+2%) and debit card (+4%) loss expense increased.
- Instant/real-time payments saw low to no losses reported.

CHART 3

Chart 3 recaps the combined insights on fraud attempts, fraud losses and the mix of fraud loss expense across payment types reported by institutions alongside industry headwinds, tailwinds and example efforts to mitigate risks.

Payment Risk Summary

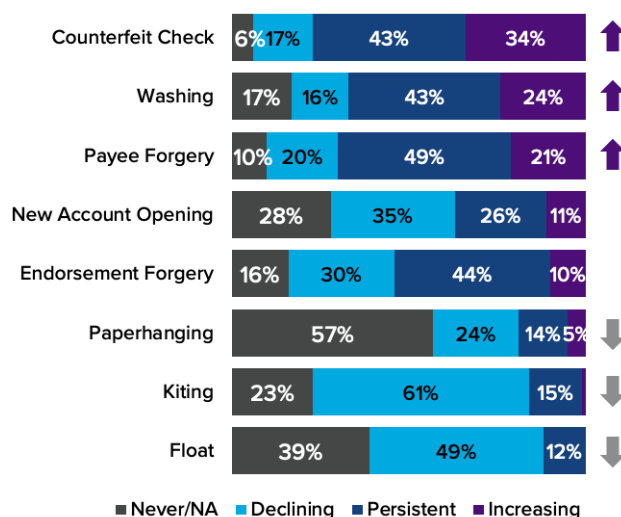


- Fraud attempts and fraud losses were most notable in debit cards and checks, with increasing attempts and losses realized. In addition to challenges with scams and mule accounts, traditional legacy fraud approaches like forgery, counterfeits, stolen mail and impersonating authorized parties were noted as primary drivers. Paper hanging, check kiting and fraud were noted as less prevalent drivers.
- While ACH saw an increase in fraud attempts, growing attempts did not have an impact on FIs experiencing losses. The number of credit card, faster payments and wire transfer fraud attempts, as well as losses realized, were perceived as flat. Instant payments fraud attempts and monetary losses were reported as negligible.

CHART 4

FI experience with counterfeit check (94%), payee forgery (90%), endorsement forgery (84%) and check washing (83%) were among the primary drivers of fraud events in 2024. FIs with check losses clarified which events were more common and describe their perception of whether an event was worsening (increasing), systemic (persistent), or improving (declining).

Specific Check Fraud Events



- Fraud events most difficult to mitigate with increasing losses included counterfeit (34%), washing (24%) and payee forgery (21%).
- Kiting (61%), float (49%) and paperhanging (24%) primarily declined, suggesting cooperative industry efforts are reducing risk and losses.

Illustrative Challenges

“Check fraud still requires additional resources to review and is more difficult to detect due to type of fraud.” (\$1B+)

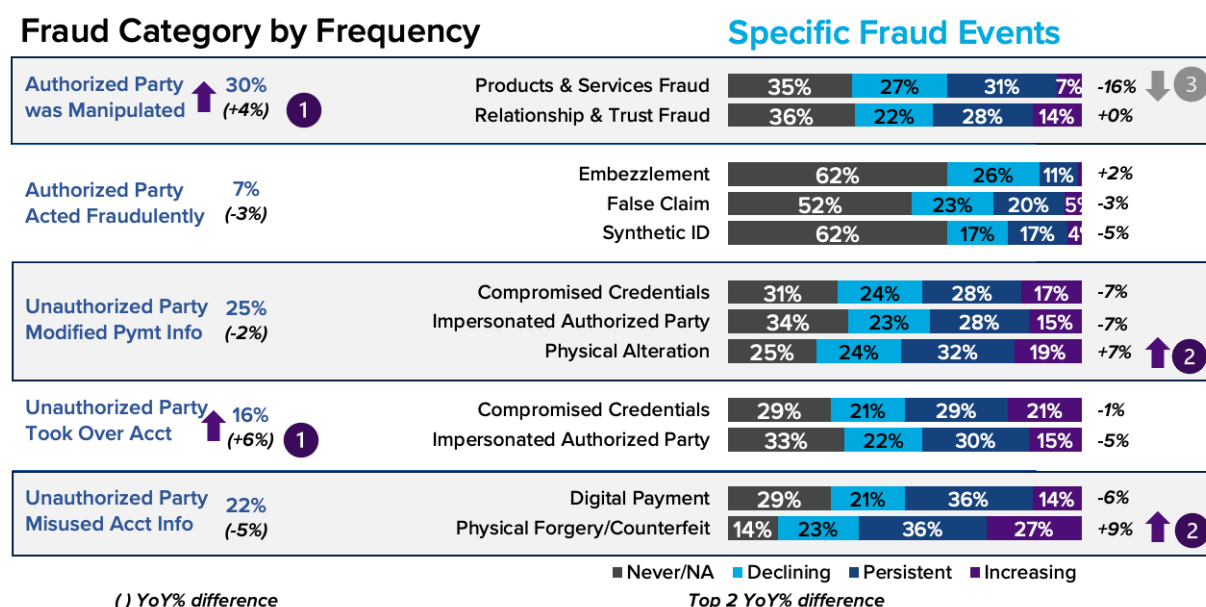
“Technology costs and resources and the ability to incorporate old school techniques for check fraud.” (\$1B+)

“Needing online and real time data to know immediately when the fraud/threats are occurring.” (\$1B+)

CHART 5

FIs perceived physical forgery/counterfeit (27%), compromised credentials (21%) and physical alteration (19%) as the top increasing fraud events, leveraging the FraudClassifierSM model for fraud types.

Fraud Frequencies and Specific Events

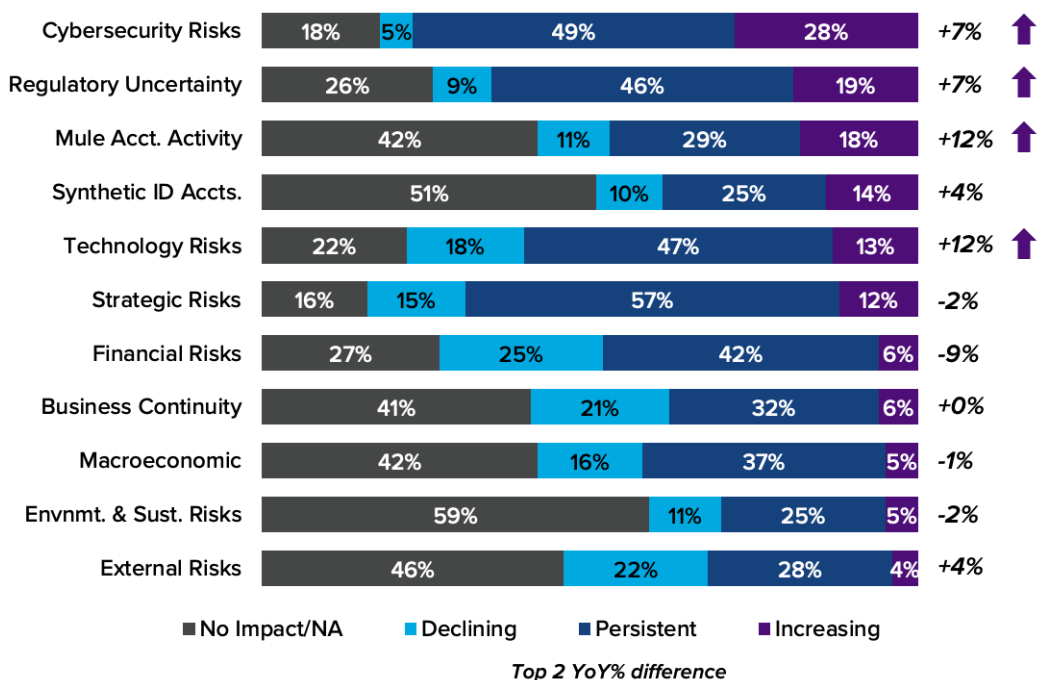


1. Top increases in fraud by frequency: FIs identified Authorized Party was Manipulated (scams) as their most common fraud 30% of the time, with a significant increase (+6%) in account takeover as the next highest increase.
2. Top increasing fraud events: Fraud events physical forgery/counterfeit (86%) and physical alteration (75%) were experienced by more FIs than any other type, and were also among the top three worsening events, with 27% and 19% of FIs describing them as increasing, respectively.
3. Top decreasing fraud event: On a positive note, the greatest area of improvement appears to be in products & services fraud, declining 16% from 2023.

CHART 6

The industry continues to see strategic, cybersecurity and technology risks as most impactful to their risk profiles.

2024 Impactful Areas on Risk Profiles



- Both technology and mule account activity (+12%) jumped as impactful areas of concern to risk profiles.
- Pressure of increasing concern was most pronounced in cybersecurity (28%), regulatory uncertainty (19%) and mule account activity (18%).

Illustrative Challenges

"With limited IT resources and increasing demand to support vulnerability and technology lifecycle management, strategic goals can't move quickly enough." (\$1B+)

"Everyone is always on social media. One bad post and it can cause a complete spiral." (\$100M-\$1B)

"Increased due diligence and knowledge are required to integrate with third parties, which causes strain and potential errors and extends the time estimated to implement." (\$100M-\$1B)

Resources

Example FRFS Ancillary Risk Tools Available to Financial Institutions

- Check (U.S. Treasury Checks): [FedDetect® Duplicate Notification for Check](#)
- Check (Commercial Checks, New 2024): [FedDetect Duplicate Notification for Check](#)
- Check: Advanced Notice Return Report: [FedPayments® Reporter Service for Check Services](#)
- ACH: [FedDetect Anomaly Notification \(frbservices.org\)](#)
- ACH: [FedPayments Insights Service \(frbservices.org\)](#)
- ACH: [FedACH® Risk Management Services \(frbservices.org\)](#)
- Funds Transfer: [FedTransaction Analyzer® \(frbservices.org\)](#)
- Instant Payments: [Fraud Control Tower \(fednowexplorer.org\)](#)
- Exception Resolution: [FedACH Exception Resolution Service \(frbservices.org\)](#)

Example Industry Collaboration

- [FraudClassifier Model | FedPayments Improvement](#)
- [About the ScamClassifierSM Model | FedPayments Improvement FedPayments Improvement](#)
- [Collaboration is Key – The Importance of Information Sharing - FedPayments Improvement](#)
- [Synthetic Identity Fraud Mitigation Toolkit | FedPayments Improvement](#)

Other references

Industry Resources

1. “Check Fraud,” American Bankers Association, <https://www.aba.com/banking-topics/risk-management/fraud/check-fraud>
2. “Check Fraud: A Practical Guide to Altered, Forged, and Counterfeit Checks for Community Bankers,” Independent Community Bankers of America, <https://www.icba.org/all-products/product-details/check-fraud-a-practical-guide-to-altered-forged-and-counterfeit-checks-for-community-bankers>
3. “Consumers,” National Credit Union Administration, <https://ncua.gov/consumers>
4. “Fraud Prevention Resources,” National Credit Union Administration, <https://ncua.gov/regulation-supervision/regulatory-compliance-resources/fraud-prevention-resources#:~:text=Credit%20union%20members%2C%20volunteers%2C%20and,electronically%20through%20the%20NCUA%27s%20website>
5. “ICBA releases new check fraud guide,” Independent Community Bankers of America, <https://www.icba.org/newsroom/news-and-articles/2024/11/22/icba-releases-new-check-fraud-guide>
6. “Jack Henry Launches Next-Generation Financial Crimes Platform,” Jack Henry, <https://www.jackhenry.com/resources/press-releases/jack-henry-launches-next-generation-financial-crimes-platform>
7. “Money Mules,” FBI, <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/money-mules>
8. “Money Mules: Protect Yourself,” American Bankers Association, <https://www.aba.com/news-research/analysis-guides/money-mules-protect-yourself>
9. “National Anti-Scam Centre joins forces with Australian Financial Crimes Exchange,” Cyber Daily, <https://www.cyberdaily.au/government/10696-national-anti-scam-centre-joins-forces-with-australian-financial-crimes-exchange>
10. “New Nacha Rules Take Aim at Credit-Push Fraud,” Nacha, <https://www.nacha.org/news/new-nacha-rules-take-aim-credit-push-fraud>
11. “Remarks at the Women in Housing and Finance Public Policy Luncheon, “The Fraud Challenge,” Office of the Comptroller of the Currency, <https://www.occ.treas.gov/news-issuances/speeches/2024/pub-speech-2024-132.pdf>
12. “Strengthening Defenses: How Somos is Helping Banks Combat Fraud,” CFCA, <https://cfca.org/strengthening-defenses-how-somos-is-helping-banks-combat-fraud/>
13. “The ABCs of Financial Crime: Consumer Education is the First Line of Defense,” PR Newswire, <https://www.prnewswire.com/news-releases/the-abcs-of-financial-crime-consumer-education-is-the-first-line-of-defense-302048246.html>
14. “U.S. Faster Payments Council Unveils Comprehensive Guideline for Instant Payment Sending Capabilities,” U.S. Faster Payments Council, <https://fasterpaymentscouncil.org/blog/14394/U-S-Faster-Payments-Council-Unveils-Comprehensive-Guideline-for-Instant-Payment-Sending-Capabilities>

15. “What Treasury Professionals Need to Know About Check Fraud,” Association for Financial Professionals, <https://www.afponline.org/training-resources/resources/articles/Details/what-treasury-professionals-need-to-know-about-check-fraud>
16. “When Synthetic Identities and Artificial Intelligence Collide,” FedPayments Improvement, <https://fedpaymentsimprovement.org/news/blog/artificial-intelligence-insights-added-to-synthetic-identity-fraud-mitigation-toolkit/>
17. “#BanksNeverAskThat,” American Bankers Association, <https://www.aba.com/advocacy/community-programs/banksneveraskthat>

Analysis

1. “2024 Fraud Insights Report,” American Bankers Association, <https://www.aba.com/news-research/analysis-guides/2024-fraud-insights-report>
2. “2024 Global Financial Crime Report,” Verafin, <https://verafin.com/nasdaq-verafin-global-financial-crime-report/>
3. “2024 Money Mule Infographic,” Nacha, https://www.nacha.org/system/files/2024-02/2024%20Money%20Mule%20Infographic_Alliance%20FINAL.pdf
4. “Check Fraud,” United States Postal Inspection Service, <https://www.uspis.gov/news/scam-article/check-fraud>
5. “Discover True Cost of Fraud Study Results,” LexisNexis Risk Solutions, <https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study>
6. “Faces of Fraud,” <https://www.sas.com/en/whitepapers/faces-of-fraud-113582.html>
7. “Financial Trend Analysis, Mail Theft-Related Check Fraud: Threat Pattern & Trend Information, February to August 2023,” Financial Crimes Enforcement Network, <https://www.fincen.gov/sites/default/files/shared/FTA-Check-Fraud-FINAL508.pdf>
8. “FinCEN Issues In-Depth Analysis of Check Fraud Related to Mail Theft,” Financial Crimes Enforcement Network, <https://www.fincen.gov/news/news-releases/fincen-issues-depth-analysis-check-fraud-related-mail-theft>
9. “Telecommunications fraud increased 12% in 2023 equating to an estimated \$38.95 billion lost to fraud,” CFCA, <https://cfca.org/telecommunications-fraud-increased-12-in-2023-equating-to-an-estimated-38-95-billion-lost-to-fraud/>
10. “The State of Synthetic Fraud: Evolution, Trends, and How We Will Eradicate it By 2026,” Socure, <https://www.socure.com/resources/reports/state-of-synthetic-fraud>
11. “Trends in Fraud for 2024 and Beyond,” Datos insights, <https://datos-insights.com/reports/trends-in-fraud-for-2024-and-beyond/>

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: 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)*

Chart 2: On estimate, what portion of your institution's payment fraud loss expenses have occurred with these payment methods in the past 12 months?

Chart 4: 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 5a: Please rank the following five types of payment fraud by frequency of occurrence in your institution over the past 12 months.

Chart 5b: 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 6: 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)*

Do you have ideas, questions, or want to learn more?

Reach out to Robert.A.Williams@chi.frb.org.

Definitions

1: Check fraud types (Chart 4)

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

2: FraudClassifier Model definitions (Chart 5)

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)

©2025 Federal Reserve Banks. The Financial Services logo, “FedACH,” “FraudClassifier,” “ScamClassifier,” “FedDetect,” “FedPayments,” “FedTransaction Analyzer,” “FedNow” and “FRBservices.org” are service marks of the Federal Reserve Banks. A list of marks related to financial services products that are offered to financial institutions by the Federal Reserve Banks is available at [FRBservices.org](https://www.frb.org/services).