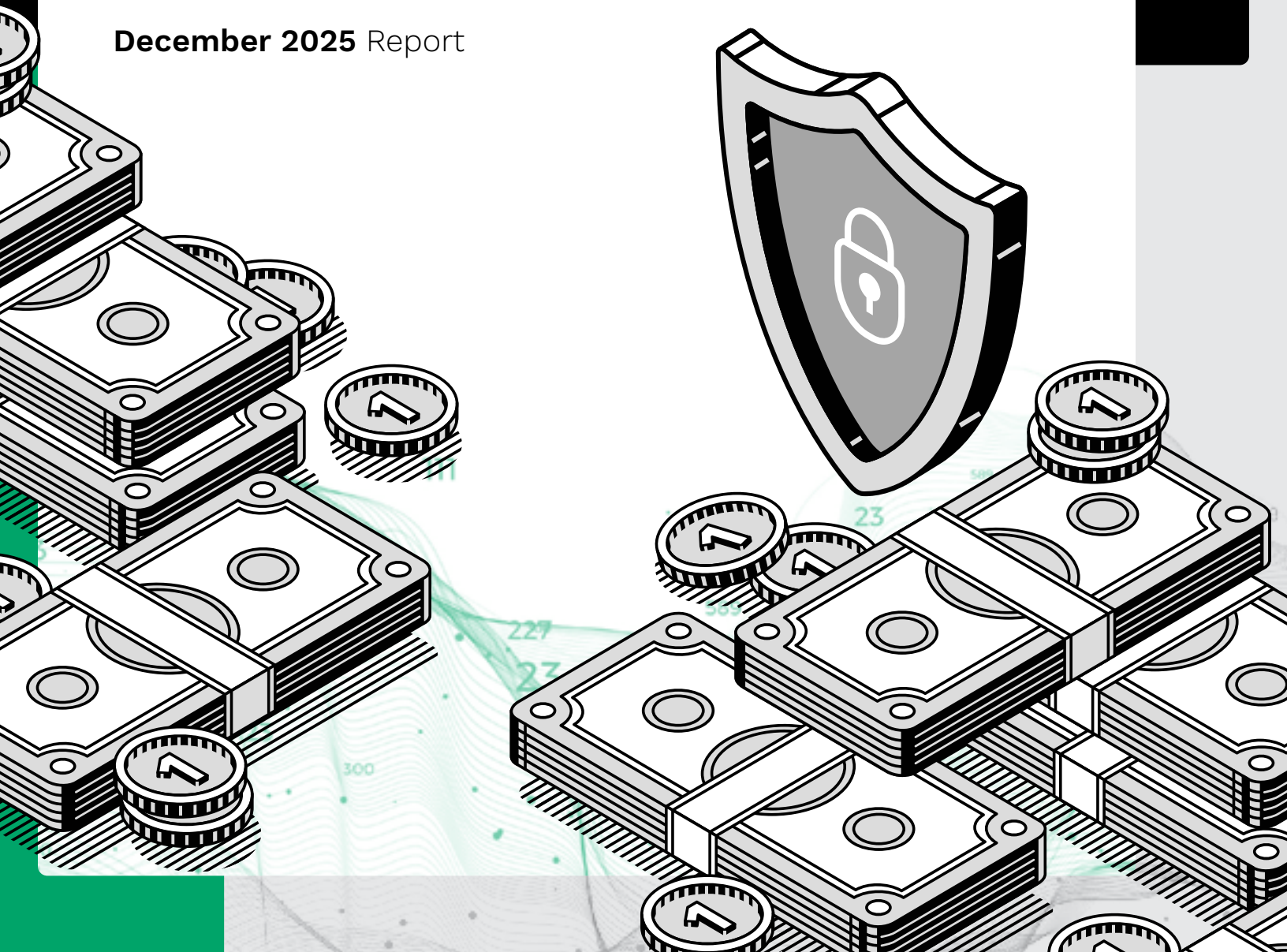


2025 STATE OF FRAUD

AND FINANCIAL CRIME IN THE UNITED STATES

December 2025 Report



2025 STATE OF FRAUD AND FINANCIAL CRIME IN THE UNITED STATES

READ MORE



November 2025
Financial Scams
and Consumer Trust

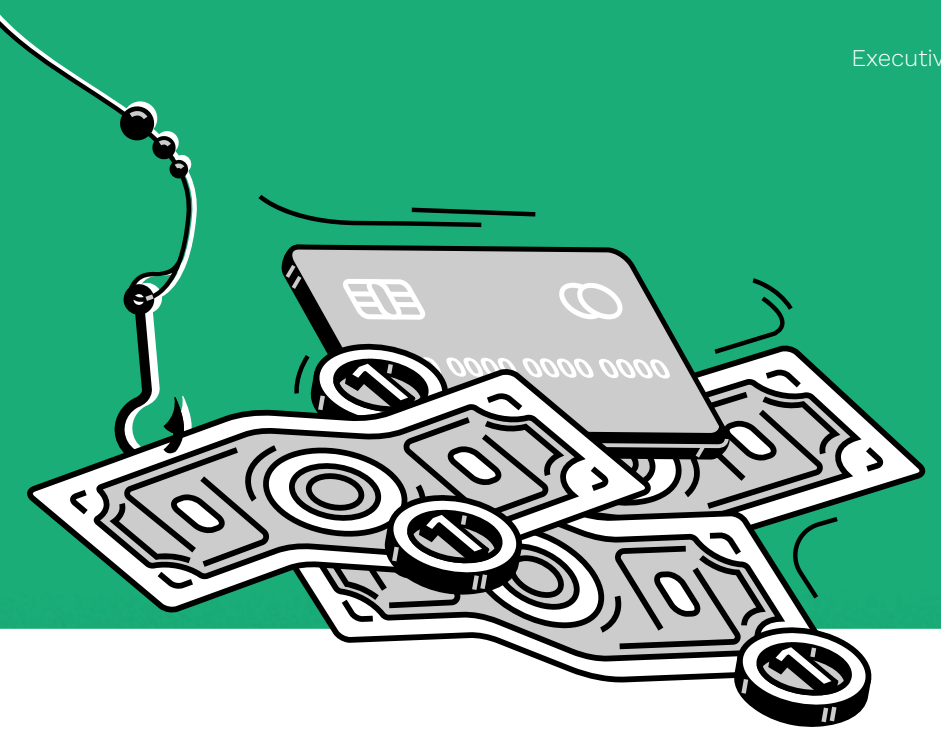
PYMNTS
INTELLIGENCE | **block**

2025 State of Fraud and Financial Crime in the United States report was commissioned by Block, and PYMNTS Intelligence is grateful for the company’s support and insight. [PYMNTS Intelligence](#) retains full editorial control over the following findings, methodology and data analysis.

TABLE OF CONTENTS

Executive Summary	4
Key Findings	6
Key Finding 01.	12
Key Finding 02	20
Key Finding 03	28
Key Finding 04	34
Key Finding 05	42
Conclusion	50
Methodology.	51
About	52

EXECUTIVE SUMMARY



The 2025 State of Fraud and Financial Crime in the United States report, produced by PYMNTS Intelligence in collaboration with Block, reveals that financial institutions are navigating a fraud environment that is increasingly sophisticated and adaptive. Unauthorized-party schemes, driven by credential theft and account takeovers, have surged, reversing last year's pattern and underscoring the dynamic nature of fraud tactics.

Average fraud loss rates rose to 0.8 basis points in 2025, with large banks reporting losses nearly four times that level. Yet the consequences extend beyond balance sheets: Half of institutions report damage to customer loyalty, and nearly as many cite reputational harm and lost business opportunities, highlighting how fraud now threatens long-term growth through its impact on trust.

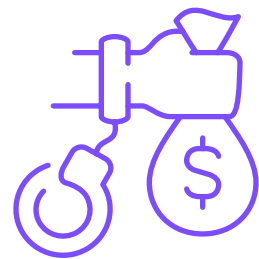
Institutions are also managing overlapping regulatory (47%) and operational (41%) pressures tied to faster, more diverse payment systems. Against this backdrop, 68% of firms increased fraud-detection spending, reflecting how technology has shifted from a discretionary expense to a strategic requirement.

The industry's next wave of modernization is being shaped by artificial intelligence and behavioral analytics, which are enabling adaptive, intelligence-driven defenses that blend proactive and reactive strategies. As financial institutions continue to modernize, investments in AI, cloud infrastructure and automation are converging into hybrid models of fraud prevention. These multilayered strategies reflect an industry steadily moving toward continuous, intelligence-led fraud prevention systems designed to meet a more complex risk environment.

KEY FINDINGS

01

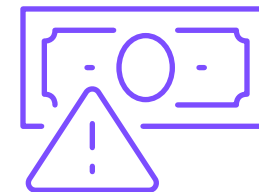
FRAUD LANDSCAPE CONTINUES TO EVOLVE AS UNAUTHORIZED-PARTY SCHEMES SURGE



Unauthorized-party fraud, driven by credential and account takeover attacks, now represents 71% of all incidents and dollar losses, reversing last year's pattern and underscoring the need for adaptive, intelligence-driven defenses.

02

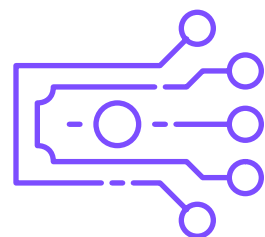
FRAUD SOPHISTICATION AND OPERATIONAL PRESSURES HIGHLIGHT A COMPLEX RISK ENVIRONMENT



A mix of increasing fraud sophistication, reported by 46% of financial institutions, along with regulatory pressures (cited by 47%) and operational pressures (with 41% citing faster or more diverse payments), underscores how financial institutions are navigating a continuously changing risk landscape.

03

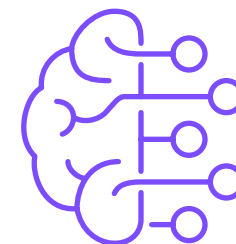
FRAUD'S IMPACT EXTENDS BEYOND FINANCIAL LOSSES, REVEALING UNEVEN PATHS TO MODERNIZATION



Beyond financial consequences, fraud challenges institutions' ability to maintain trust and brand integrity, as barriers to innovation reveal disparities across institution types.

04

AI AND ADVANCED BEHAVIORAL ANALYTICS DEFINE MODERN FRAUD DEFENSE, YET GAPS PERSIST ACROSS INSTITUTIONS



The widespread integration of AI and modern behavioral analytics marks their evolution from emerging tools to baseline capabilities, even as one in five financial institutions, particularly smaller and regional banks, still operate without them.

05

AI IS RESHAPING FRAUD STRATEGIES AND DRIVING THE NEXT WAVE OF MODERNIZATION



Machine learning is enabling institutions to balance proactive and reactive defenses, while future investments involve AI, cloud infrastructure and improved customer communication.



KEY FINDING



01

Fraud Landscape Continues to Evolve as Unauthorized-Party Schemes Surge.

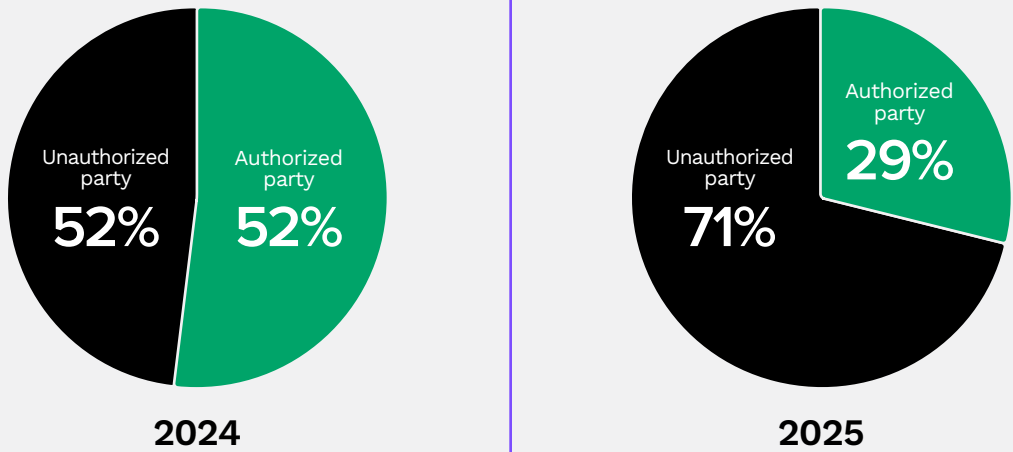
Unauthorized-party fraud, driven by credential and account takeover attacks, now represents the majority (71%) of total incidents and dollar losses. This reverses last year's pattern, in which 48% of fraud incidents were initiated by unauthorized parties, underscoring the need for adaptive, intelligence-driven defenses.

Fraud Landscape Remains Dynamic as the Proportion of Incidents Involving Unauthorized Access Increases

The 2025 fraud landscape underscores how dynamic and adaptive financial crime has become. The proportion of total fraud involving unauthorized-party access increased across both total transactions and dollar value, reversing 2024’s pattern when most incidents stemmed from authorized-party manipulation. This shift signals a resurgence of external fraud in which bad actors exploit credentials, accounts, or payment information to initiate unauthorized activity. The findings highlight the continuously evolving nature of fraud and the growing need for financial institutions to adopt proactive, intelligence-driven defenses.

Fraud remains a moving target, driven by the continual interplay between fraudsters and financial institutions. As fraudster refine tactics to exploit emerging vulnerabilities, institutions adapt their defenses through new technologies, analytics, and operational strategies. This reciprocal evolution underscores that fraud prevention is not static, but instead a dynamic contest of innovation on both sides.

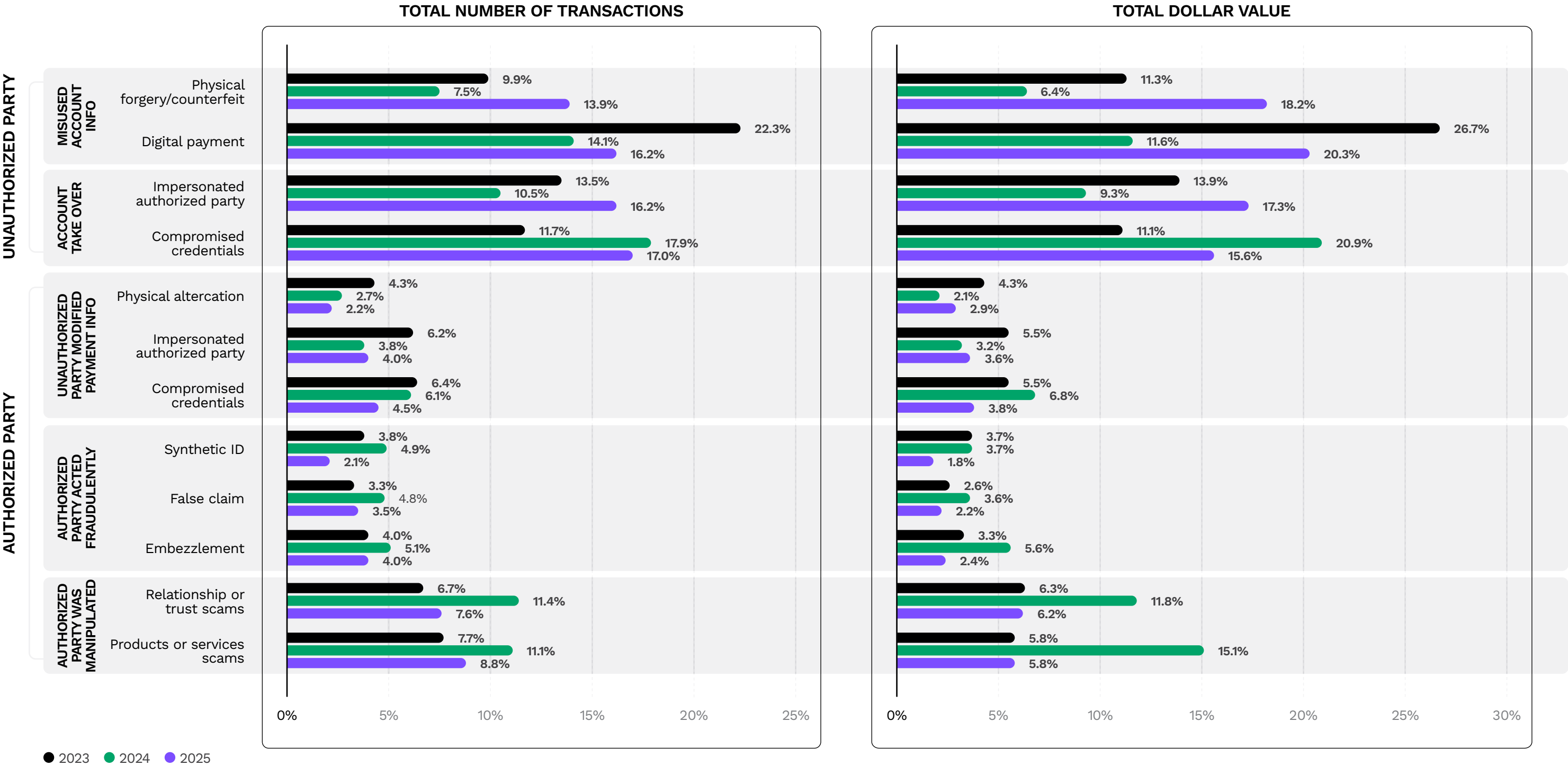
FIGURE 1:
Share of Fraud Losses by Party Type
Percentage of total fraud losses classified as authorized-party versus unauthorized-party incident



Source: PYMNTS Intelligence
2025 State of Fraud and Financial Crime in the United States, December 2025
N = 200: Complete executive sample, fielded Sept. 30, 2025, to Oct. 15, 2025

FIGURE 2:
Share of Fraud and Scam Types by Number of Transactions and Dollar Value
Distribution of total transactions and total dollar value across fraud and scam types involving unauthorized and authorized parties

Source: PYMNTS Intelligence
2025 State of Fraud and Financial Crime in the United States, December 2025
N = 200: Complete executive sample, fielded Sept. 30, 2025, to Oct. 15, 2025

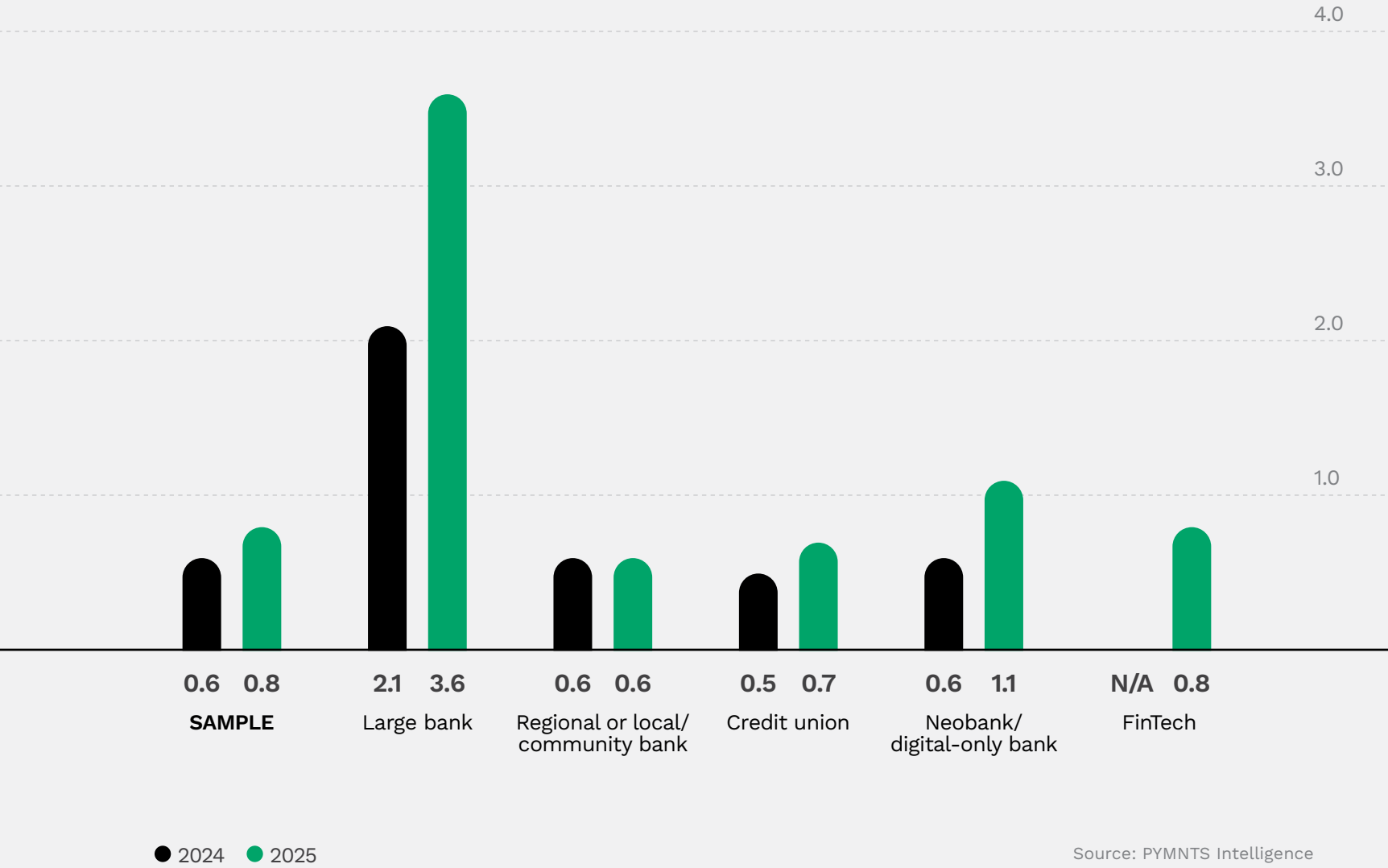


Loss Rates Edge Up, Driven by Large Banks and Neobanks

Across the industry, fraud loss rates averaged 0.8 basis points over the past 12 months, a modest increase from 0.6 basis points in 2024. This persistence of losses signals a continuing equilibrium: Despite evolving fraud tactics and new institutional defenses fraud continues to be a persistent and significant problem. Yet these averages mask sharp disparities. Large banks report losses exceeding 3.5 basis points, more than four times the industry average in our survey sample, while Fin-Techs and smaller and regional institutions remain closer to 0.6–0.7. Neobanks and also report above-average loss rates, reflecting the operational exposure that accompanies speed and scale.

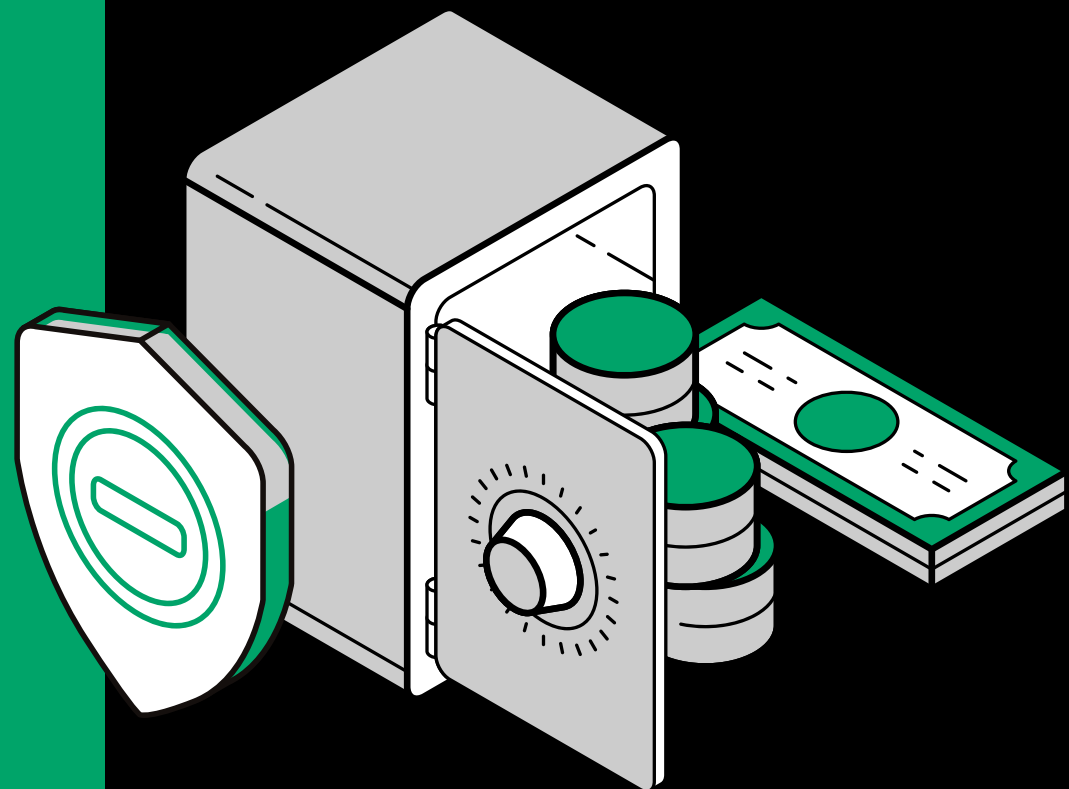
The modest uptick in losses shows the ongoing impact of fraud on financial institutions. Fraudsters continue to adapt as quickly as institutions counter them, creating a fragile equilibrium that masks growing pressure on large, fast-moving banks.

FIGURE 3:
Fraud Loss Rate by Institution Type (in Basis Points)
Fraud losses as a percentage of total transactions over the past 12 months, reported by each institutional segment



Source: PYMNTS Intelligence
2025 State of Fraud and Financial Crime in the United States, December 2025
N = 200: Complete executive sample, fielded Sept. 30, 2025, to Oct. 15, 2025

KEY FINDING



02

Fraud Sophistication and Operational Pressures Highlight a Complex Risk Environment.

A mix of increasing fraud sophistication, reported by 46% of financial institutions, along with regulatory pressures (cited by 47%) and operational pressures (with 41% citing faster or more diverse payments), underscores how financial institutions are navigating a continuously changing risk landscape.

Rising Fraud Sophistication Reframes Technology as Essential Infrastructure

Nearly half of financial institutions (46%) report that the sophistication of fraud schemes has increased sharply over the past year, up from 35% in 2024, adding pressure on existing defenses. At the same time, the share of firms citing cost as a barrier to adopting new fraud-prevention technology declined from 60% to 36%, indicating a marked reduction in cost sensitivity. This reduction may reflect multiple factors, including changes in financial institutions’ priorities, greater availability of lower-cost or easier-to-implement tools and broader industry familiarity with modern solutions.

While these trends do not imply direct causation, they collectively point to a changing operational environment: Institutions face more complex fraud while simultaneously becoming more willing to invest in technology as a strategic requirement.

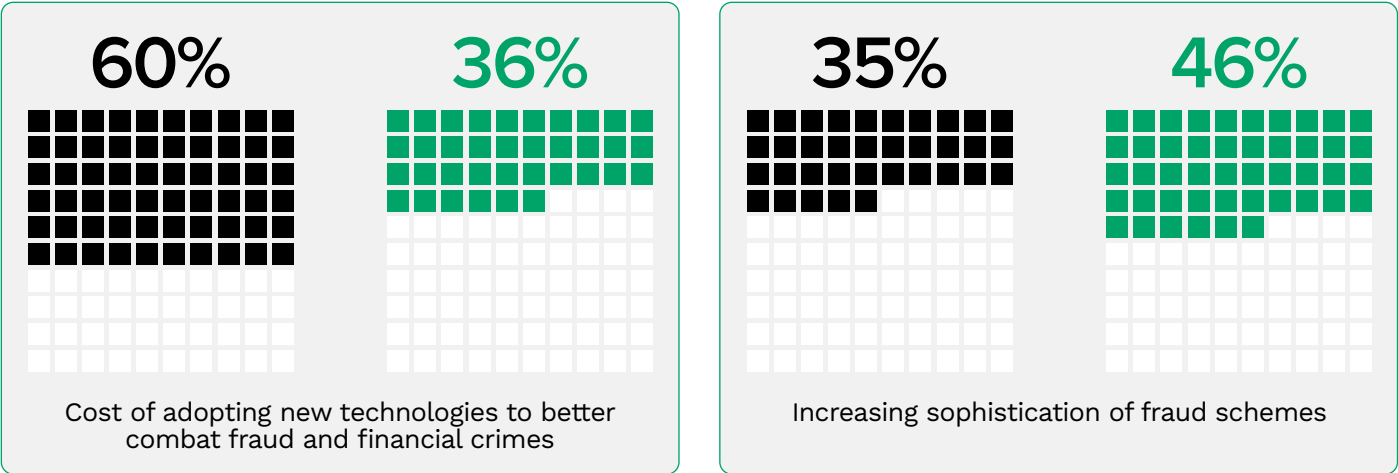
Reflecting this shift in priorities, 68% of financial institutions increased their fraud-detection budgets year over year, underscoring the industry’s continued movement toward proactive, technology-driven defense.

Parallel trends in fraud sophistication, cost perception and investment highlight an industry in transition. Rising sophistication and changing cost perceptions coincide with continued increases in fraud-detection spending, indicating that modernization remains an active focus across institutions.

68%

of financial institutions report **increasing their fraud detection spending YoY.**

FIGURE 4:
Key Fraud-Related Challenges Cited by Financial Institutions
Percentage of institutions identifying each factor as a primary challenge, year over year



● 2024 ● 2025

Source: PYMNTS Intelligence
2025 State of Fraud and Financial Crime in the United States, December 2025
N = 200: Complete executive sample, fielded Sept. 30, 2025, to Oct. 15, 2025

As Fraud Grows More Complex, Financial Institutions Confront a Multitude of Pressures

Financial institutions face a broad mix of fraud and compliance pressures that extend beyond traditional external attacks. Nearly half (46%) cite rising fraud sophistication, but many also point to challenges driven by customer behavior, including 39% who say customers are increasingly willing to engage in third-party fraud.

Operational demands add further strain. Institutions must manage expanding regulatory requirements (47% cite sanctions compliance), faster payment speeds (46%) and greater diversity in payment types and currencies (41%). At the same time, institutions continue to navigate technology limitations, including integration with legacy systems and the need for solutions that can identify and block fraud in real time. Taken together, these pressures illustrate an environment in which institutions must balance fraud risk, compliance obligations and payment-system modernization simultaneously, often within complex, interconnected systems.

46%

of financial institutions report **increasing sophistication in fraud schemes.**

The takeaway is clear: Financial institutions face simultaneous challenges from external attackers, customer-driven fraud, expanding regulation and rapid payment innovation, all of which stretch fraud-prevention approaches.

Confronted with smarter fraud schemes, strict regulation, and a payments landscape evolving in real time, financial institutions are reaching an inflection point. The conversation has shifted from “Can we afford this?” to “Can we afford not to?”

FIGURE 5:
Challenges Financial Institutions Face in Managing Fraud
Share of financial institutions reporting each challenge, by institution type

		SAMPLE	FinTech	Neobank/ digital-only bank	Credit union	Regional or local/ community bank	Large bank
EVOLVING EXTERNAL THREATS	Increasing sophistication of fraud schemes	46%	49%	39%	44%	48%	27%
	Customer to engage in third-party fraud	39%	33%	23%	39%	46%	29%
	Increasing number of fraud and financial crimes	39%	49%	36%	45%	33%	32%
	Cyber and data breaches	34%	28%	53%	28%	36%	9%
FINANCIAL IMPACT	Cost to the bank for reimbursing fraud-related losses	46%	42%	50%	42%	48%	41%
	Cost of adopting new technologies to better combat fraud and financial crimes	36%	37%	32%	44%	33%	41%
	Loss of customers and revenues due to fraud and financial crimes	36%	30%	21%	49%	37%	25%
REGULATORY COMPLIANCE	Financial sanctions compliance	47%	42%	51%	34%	53%	82%
	Complex regulatory requirements	45%	44%	33%	53%	45%	52%
TECHNOLOGICAL LIMITATIONS	Increased speed of payments	46%	40%	65%	34%	49%	70%
	Expansion of payment types or currencies, including peer to peer, instant transactions, cryptocurrencies	41%	40%	54%	38%	41%	41%
	Inability of our system to integrate with new solutions to identify and block fraud and financial crimes	35%	37%	24%	38%	34%	50%
	Inability of our current solutions to identify fraudulent transactions	32%	33%	40%	36%	29%	25%
Organizational design		28%	21%	39%	22%	31%	43%

Source: PYMNTS Intelligence
2025 State of Fraud and Financial Crime in the United States December 2025
N = 200: Complete executive sample, fielded Sept. 30, 2025, to Oct. 15, 2025

KEY FINDING



03

Fraud’s Impact Extends Beyond Financial Losses, Revealing Uneven Paths to Modernization.

Beyond financial consequences, fraud challenges institutions’ ability to maintain trust and brand integrity, as barriers to innovation reveal disparities across institution types.

Fraud’s Impact Reaches Beyond the Balance Sheet

Fraud’s impact extends well beyond financial losses, influencing how institutions sustain trust and continuity. Half of financial institutions (50%) report a negative effect on customer loyalty, while 44% cite brand damage and 48% have lost new business opportunities. Nearly as many (47%) experienced operational disruptions linked to fraud, with 36% saying these experiences underscored the need for new technologies to restore resilience and reinforce readiness. Together, these outcomes reveal how fraud reverberates through financial, reputational, and operational dimensions of institutional performance.

Fraud’s true cost is measured in trust and opportunity as much as in dollars. Beyond direct losses, institutions face lasting effects on loyalty, reputation, and growth, highlighting that strengthening fraud protection also strengthens confidence in the systems that sustain it.

FIGURE 6:
How Fraud Affects Financial Institutions
Percentage of financial institutions reporting the following challenges in combatting fraud and financial crimes, segmented by institution type

		SAMPLE	FinTech	Neobank/ digital-only bank	Credit union	Regional or local/ community bank	Large bank
CUSTOMER AND BRAND IMPACT	Negative impact on customer loyalty	50%	49%	34%	42%	59%	48%
	Damage to our brand and reputation	44%	40%	51%	41%	46%	50%
DIRECT FRAUD OUTCOMES	Increased incidents of fraud	49%	42%	34%	61%	51%	52%
FINANCIAL AND OPERATIONAL IMPACT	Lost new business opportunities	48%	49%	34%	50%	49%	59%
	Financial losses	47%	44%	24%	53%	52%	57%
	Operational disruptions or failures	47%	56%	70%	33%	43%	47%
INTERNAL ORGANIZATIONAL IMPACT	Highlighted the need to adopt new technologies to combat fraud	36%	35%	63%	46%	26%	18%
	Lowered employee moral	34%	42%	28%	21%	37%	57%
OTHER	Regulatory actions	31%	28%	11%	53%	28%	39%

Source: PYMNTS Intelligence
2025 State of Fraud and Financial Crime in the United States, December 2025
N = 200: Complete executive sample, fielded Sept. 30, 2025, to Oct. 15, 2025

One Size Doesn’t Fit All: Different Institutions Face Different Innovation Hurdles

Barriers to innovation in fraud prevention vary sharply by institution type, reflecting differences in scale, infrastructure, and strategic priorities. On average, financial institutions report facing 3.9 distinct barriers to modernization. Large banks most often cite competing innovation demands (66%) and integration challenges (66%), while regional banks and credit unions point to higher data management costs (62% and 55%). FinTechs, by contrast, struggle more with technology complexity (60%) as they balance speed and scalability. These differences show that while the drive to modernize is widespread, the ability to do so efficiently depends on each institution’s structure and capacity.

The road to modernization isn’t uniform. Each institution must balance ambition, resources, and risk appetite to build fraud defenses suited to its scale, systems, and strategic priorities.



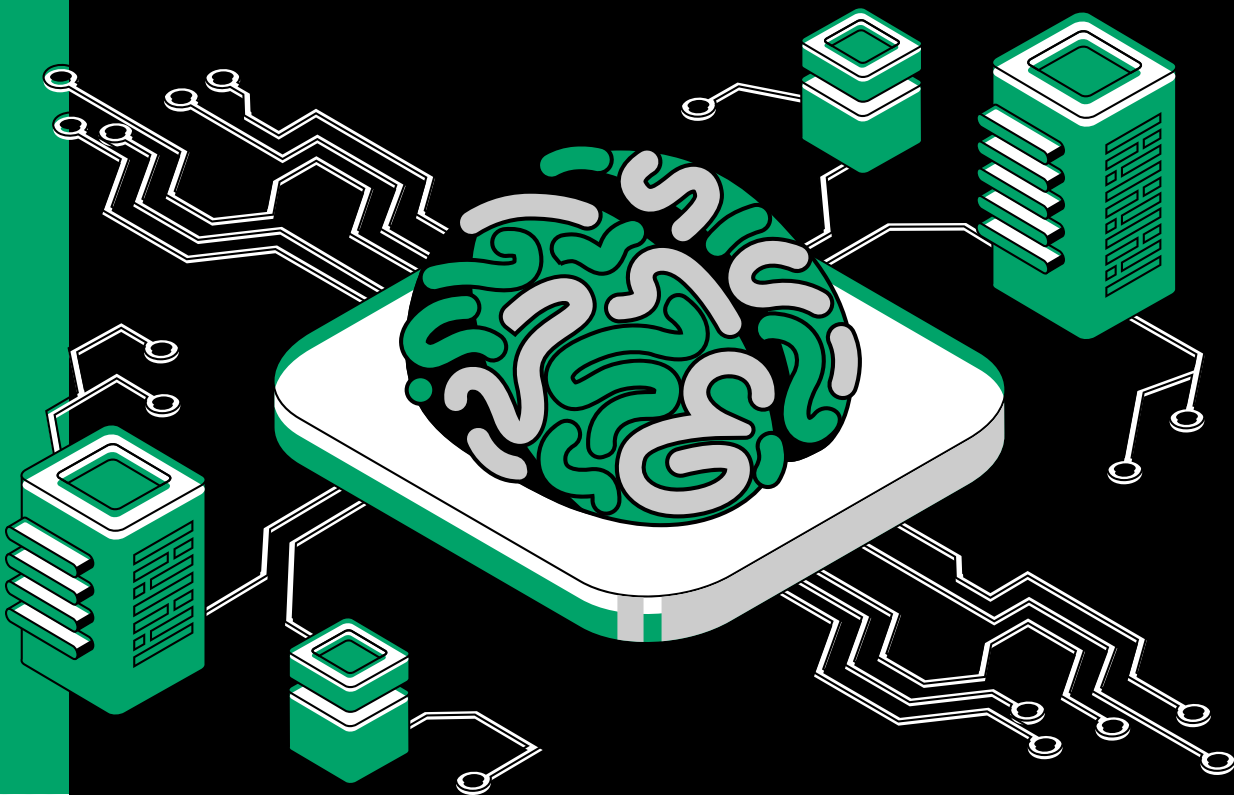
Financial institutions reported **3.9 barriers to innovation** on average.

FIGURE 7:
Barriers to Innovation in Fraud Prevention
Share of financial institutions reporting each barrier, segmented by institution type

	SAMPLE	FinTech	Neobank/ digital-only bank	Credit union	Regional or local/ community bank	Large bank
Higher data management costs associated with new technology systems	53%	37%	43%	55%	62%	61%
Higher priority given to other areas of innovation	52%	40%	56%	64%	50%	66%
Cost of the innovation	51%	51%	49%	49%	53%	52%
Complexity of using new technology systems	48%	60%	45%	32%	52%	36%
Difficulties integrating new solutions to our existing systems	47%	49%	33%	70%	38%	66%
Available technology	42%	44%	55%	46%	36%	32%
Regulatory constraints or difficulties	39%	33%	35%	41%	43%	50%

Source: PYMNTS Intelligence
2025 State of Fraud and Financial Crime in the United States, December 2025
N = 200: Complete executive sample, fielded Sept. 30, 2025, to Oct. 15, 2025

KEY FINDING



04

AI and Advanced Behavioral Analytics Define Modern Fraud Defense, Yet Gaps Persist Across Institutions.

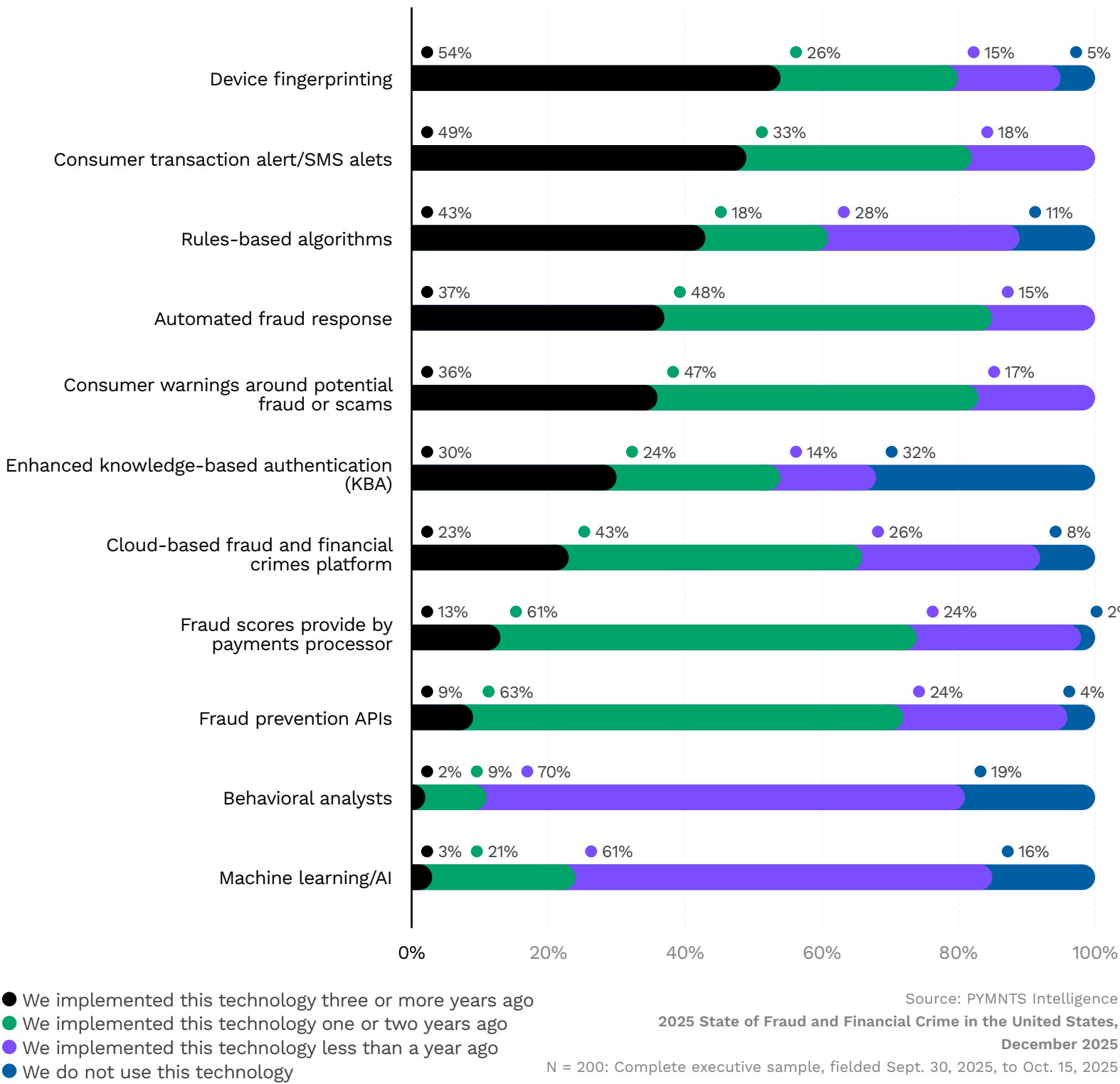
The widespread integration of AI and modern behavioral analytics tools marks their evolution from emerging tools to baseline capabilities, even as one in five financial institutions, particularly smaller and regional banks, still operate without them.

Machine Learning and Behavioral Analytics Gain Broader Integration in Fraud Defense

Over the past year, financial institutions have expanded their use of intelligent, data-driven technologies to strengthen fraud defenses. Machine learning (61%) and behavioral analytics (70%) were the most frequently reported additions in 2025, reflecting both new deployments and the formal integration of behavior-based methods within existing fraud systems. This broadening use signals a shift toward adaptive, intelligence-driven detection strategies capable of identifying subtle and evolving fraud behaviors in real time, complementing, rather than replacing, traditional rules-based approaches.

Behavioral analytics and machine learning are becoming foundational, not just experimental. Their expanding use marks the maturation of intelligence-driven defense, transforming fraud prevention from a rules-based process into an adaptive, enterprise-level capability.

FIGURE 8:
Technologies Financial Institutions Use to Combat Fraud
Percentage of financial institutions adopting each tool



FinTechs and Large Banks Near Full Adoption of AI and Behavioral Analytics

FinTechs and large banks report near-universal use of AI and advanced behavioral analytics, reflecting the mature integration of intelligence-based fraud defenses. In 2025, roughly eight in 10 FinTechs (79%) and large banks (77%) report implementing some form of modern behavioral analytics, while adoption or enhancement of machine learning and AI stands at 65% among FinTechs and 75% among large banks. Credit unions show a comparable level of advanced behavioral analytics adoption (79%), though 13% report not using the technology. Still, nearly one in five institutions, particularly smaller and regional banks, report not using behavioral analytics, while 15% say they do not use machine learning, underscoring the modernization gap driven by legacy systems and integration hurdles.

Roughly
8 in 10

FinTechs and large banks report **implementing some form of advanced behavioral analytics tools.**

AI and behavioral analytics have become foundational in modern fraud defense. Yet nearly one in five institutions still operate without them, revealing a growing divide between technology-forward organizations and those constrained by legacy systems.

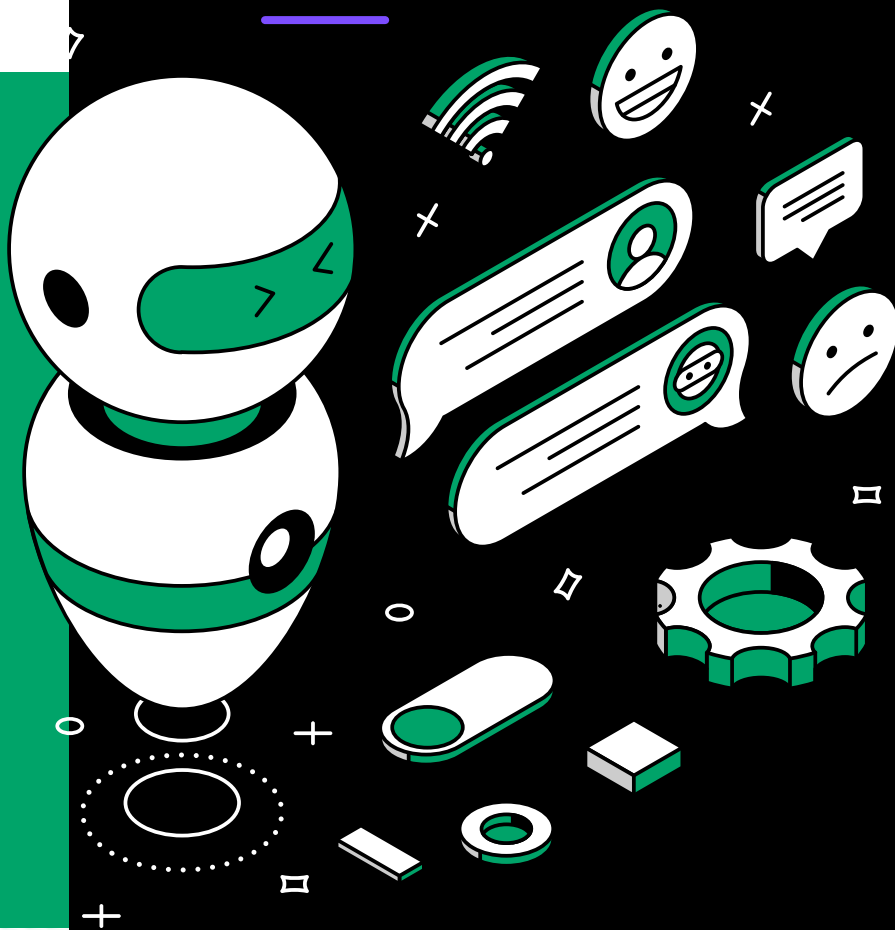
FIGURE 9:
Adoption of Behavioral Analytics and Machine Learning in Fraud Prevention
Share of financial institutions using each technology and how recently it was implemented, segmented by institution type



● We implemented this technology three or more years ago
● We implemented this technology one or two years ago
● We implemented this technology less than a year ago
● We do not use this technology

Source: PYMNTS Intelligence
2025 State of Fraud and Financial Crime in the United States
N = 200: Complete executive sample, fielded Sept. 30, 2025, to Oct. 15, 2025

KEY FINDING



05

AI Is Reshaping Fraud Strategies and Driving the Next Wave of Modernization.

Machine learning is enabling institutions to balance proactive and reactive defenses, while future investments involve AI, cloud infrastructure and improved customer communication.

Machine Learning Blends Proactive and Reactive Strategies in Fraud Defense

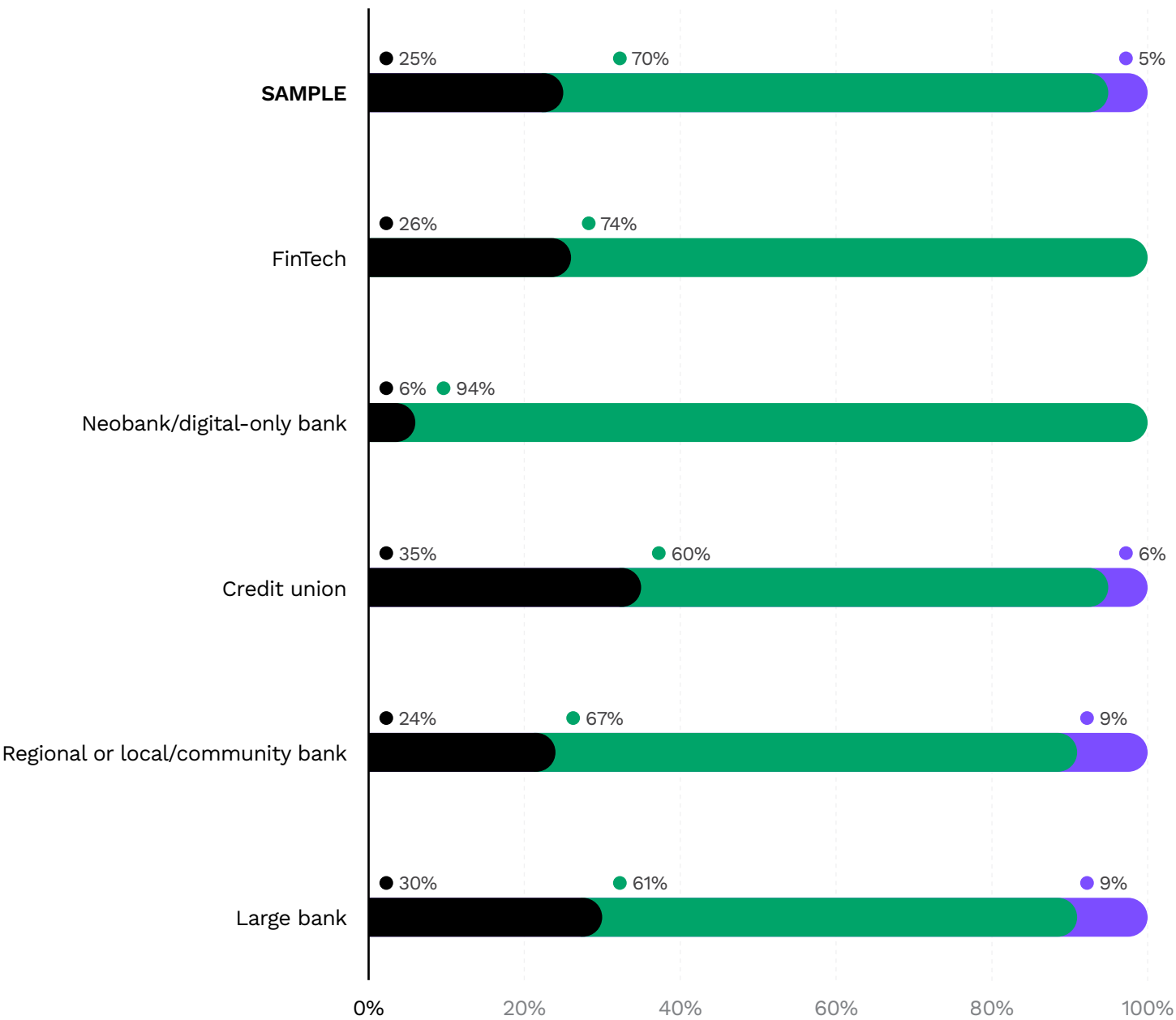
Machine learning is reshaping how financial institutions manage fraud by enabling a more integrated approach to prevention and response. Most institutions (70%) report that AI allows them to balance both proactive and reactive strategies, combining real-time detection with faster mitigation. Another 25% say AI makes them pre-dominantly more proactive overall, while a small share (5%) report it primarily strengthens reactive capabilities.

These responses reflect how institutions view the role of AI—as a technology that broadens their toolkit, enhances real-time decisioning and improves their ability to both anticipate and respond to fraud.

FIGURE 10:

Role of Machine Learning in Fraud Prevention and Response

Financial institutions reporting how machine learning is primarily used to combat fraud and financial crimes



- We implemented this technology three or more years ago
- We implemented this technology one or two years ago
- We implemented this technology less than a year ago

Source: PYMNTS Intelligence
2025 State of Fraud and Financial Crime in the United States,
December 2025

N = 200: Complete executive sample, fielded Sept. 30, 2025, to Oct. 15, 2025

Evolving Fraud Threats Drive Multilayered Investment Strategies

Financial institutions are deploying a blend of solutions to strengthen fraud defenses, signaling that no single strategy is sufficient. Roughly half plan to expand outsourcing (51%) and cloud-based fraud platforms (50%), while 44% are developing new in-house systems.

At the same time, 40% are investing in deep learning and 37% in machine learning, reflecting continued commitment to intelligence-driven detection. (Although deep learning is technically a subset of machine learning, respondents appear to view both as distinct initiatives within their broader technology roadmaps.) This diversification highlights a maturing approach to fraud prevention, where collaboration, technology, and human oversight intersect to sustain resilience across a complex threat environment.

Together, these actions point to a diversified modernization strategy, where institutions expand infrastructure, enhance internal tools and adopt advanced analytics to keep pace with evolving fraud threats. Fraud prevention now relies on a mix of external expertise, cloud capabilities and internal innovation, creating more flexible and resilient capabilities.



FIGURE 11:
Planned Enhancements to Fraud-Prevention Capabilities
Share of financial institutions planning to take the following actions to improve their existing solutions for fraud and financial crime

	SAMPLE	FinTech	Neobank/ digital-only bank	Credit union	Regional or local/ community bank	Large bank
Outsourcing the detection and prevention of fraud and financial crimes to a third party	51%	53%	30%	55%	55%	43%
Initiating or increasing the use of cloud-based fraud and financial crimes platforms	50%	40%	49%	56%	53%	39%
Developing new in-house systems for fraud and financial crimes	44%	44%	44%	51%	41%	52%
Improved communication with customers	41%	33%	65%	33%	43%	46%
Initiating or increasing the use of deep learning systems	40%	28%	57%	40%	41%	41%
Initiating or increasing the use of machine learning/AI models	37%	44%	28%	13%	48%	46%

Source: PYMNTS Intelligence
2025 State of Fraud and Financial Crime in the United States, December 2025
N = 200: Complete executive sample, fielded Sept. 30, 2025, to Oct. 15, 2025

CONCLUSION

Fraud will continue to evolve as quickly as the systems designed to stop it. The next phase of defense will require institutions to move beyond detection toward prediction, leveraging artificial intelligence, behavioral analytics and real-time data to anticipate risk before it materializes. Those that succeed will pair technological innovation with human judgment, transforming fraud prevention into an adaptive, learning ecosystem. Collaboration across financial institutions, technology providers and regulators will be essential to stay ahead of increasingly networked and intelligent fraud schemes. As financial crime grows more sophisticated, the balance between innovation and resilience will define leadership. Ultimately, protecting trust in the digital economy depends not on keeping pace with fraud, but on outpacing it.

METHODOLOGY

The 2025 State of Fraud and Financial Crime in the United States report, produced in collaboration with Block (Cash App) and PYMNTS Intelligence, is based on a survey of 200 executives working at U.S. financial institutions with assets of at least \$1 billion and at FinTechs with at least \$100 million in annual revenues in 2024. It was conducted from Sept. 30, 2025, to Oct. 15, 2025. To ensure representativeness, we weighted all bank and credit union responses by national asset-size distribution. This prevents the results from being driven by a small number of large banks and ensures that each institution type reflects its footprint in the U.S. financial system. The respondents were required to have deep knowledge and leadership responsibilities in: compliance and operations, fraud and risk operations, fraud analysis, fraud strategy, or trust and safety analyst or operations. All insights reflect PYMNTS' independently collected, double-blind survey data and analysis. It's possible that Block was surveyed, but neither PYMNTS nor Block would have known, removing the potential for bias.

THE PYMNTS INTELLIGENCE TEAM THAT PRODUCED THIS REPORT:

Lynnley Browning
Managing Editor

Matthew Albrecht, PhD
Senior Research Analyst

Ignacio Marquez
Research Analyst

ABOUT

DISCLAIMER ■

PYMNTS INTELLIGENCE

[PYMNTS Intelligence](#) is a leading global data and analytics platform that uses proprietary data and methods to provide actionable insights on what's now and what's next in payments, commerce and the digital economy. Its team of data scientists include leading economists, econometricians, survey experts, financial analysts and marketing scientists with deep experience in the application of data to the issues that define the future of the digital transformation of the global economy. This multi-lingual team has conducted original data collection and analysis in more than three dozen global markets for some of the world's leading publicly traded and privately held firms.

■ block

[Block, Inc.](#) (NYSE: XYZ) builds technology to increase access to the global economy. Each of our brands unlocks different aspects of the economy for more people. **Square** makes commerce and financial services accessible to sellers. **Cash App** is the easy way to spend, send, and store money. **Afterpay** is transforming the way customers manage their spending over time. **TIDAL** is a music platform that empowers artists to thrive as entrepreneurs. **Bitkey** is a simple self-custody wallet built for bitcoin. **Proto** is a suite of bitcoin mining products and services. Together, we're helping build a financial system that is open to everyone.

2025 State of Fraud and Financial Crime in the United States may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.

Components of the content original to and the compilation produced by PYMNTS is the property of PYMNTS and cannot be reproduced without its prior written permission.

We are interested in your feedback on this report. If you have questions, comments or would like to subscribe, please email us at feedback@pymnts.com.