datos INSIGHTS

November 2024

Trust in the Digital Age: Preparing for Tomorrow's Fraud Threats Today

Jim Mortensen and David Barnhardt

Prepared for:

Early Warning®

November 2024

Trust in the Digital Age: Preparing for Tomorrow's Fraud Threats Today

Jim Mortensen and David Barnhardt

Table of Contents

List of Figures

List of Tables

Executive Summary

The landscape of fraud in banking is evolving at an unprecedented pace, driven by technological advancements and the increasing sophistication of fraudsters. As financial institutions (FIs) race to fortify their defenses, they face a complex array of challenges, from traditional fraud schemes to emerging threats powered by artificial intelligence.

Datos Insights surveyed fraud executives at 75 FIs and conducted multiple in-depth interviews with other fraud prevention experts to gain insight into this dynamic environment. This dual approach enabled a panoramic view of the current state of fraud in banking, emerging trends, and the strategic investments institutions are making to stay ahead of fraudsters. The research unveils a sector in transition, grappling with persistent familiar and novel fraud threats, and highlights the critical importance of adaptive strategies and innovative technologies in maintaining the integrity of financial systems in the digital age. The following are the key findings:

- Card-not-present (CNP) fraud and first-party application fraud emerge as the most prevalent attack types, with 65% of surveyed institutions reporting CNP fraud as a top concern.
- Social engineering payment scams and synthetic identity fraud show significant increases, with 59% and 63% of institutions reporting rises in these areas, respectively.
- Generative artificial intelligence (GenAI) is perceived as a major emerging threat, with 93% of institutions expressing concern about defending against AI-powered attacks.
- Investment priorities focus on digital identity authentication (55% of FIs) and identity verification controls (43% of FIs), reflecting the critical nature of these defenses in the digital banking era.
- FIs are balancing fraud prevention with customer experience, with 88% agreeing that customer experience is equally important to fraud loss control.

As the financial landscape continues to evolve, institutions that can effectively adapt to these changing threats will be best positioned to protect their assets and maintain customer trust in an increasingly digital world.

Introduction

The digital transformation of financial services is ushering in an era of unprecedented convenience for consumers. Mobile banking, instant payments, and online account opening have revolutionized the way people interact with their FIs. However, this digital evolution has also carved out new avenues for sophisticated fraud attacks. As technology advances, fraudsters adapt and evolve their methods, creating a perpetual challenge for FIs to safeguard their assets and protect their customers across all product lines.

In this rapidly changing landscape, staying ahead of emerging threats is a critical priority for banks and credit unions. The fraud prevention arms race spans the entire spectrum of financial products, from traditional checking and savings accounts to credit and debit cards to cutting-edge payment technologies and digital lending platforms.

Each innovation in financial services brings with it new vulnerabilities that fraudsters are quick to exploit. At the same time, older payment mechanisms such as checks persist with their own set of fraud challenges.

FIs must maintain a comprehensive understanding of the current fraud landscape while anticipating future threats to navigate this complex terrain. Core to this effort is developing fraud prevention frameworks that adapt as the threat fabric evolves. This report and the underlying research delve into the heart of these challenges, examining prevalent attack types, emerging trends, and the strategic investments institutions are making to fortify their defenses. It provides a window into the state of fraud in banking today and provides a roadmap for preparing against tomorrow's threats.

As FIs continue to innovate and expand their digital offerings, consideration of the insights and strategies outlined within this report will be crucial in maintaining trust, security, and resilience in the face of ever-evolving fraud threats.

Methodology

This report is largely based on data from a Datos Insights online survey conducted of fraud prevention leaders at 75 U.S. FIs, complemented by multiple interviews. The survey was designed to elicit information about the institutions' current fraud prevention practices and strategies, emerging fraud trends, investment priorities, and perspectives on the use of AI in fraud perpetration and prevention.

The sample of FIs represents a cross-section of the U.S. banking industry, including large national banks, smaller regional institutions, and credit unions. A survey of this size offers a 10-point margin of error at a 90% confidence level; statistical tests for differences between segments were conducted at a 90% level of confidence.

Threat Intelligence: How Fraud Attacks Are Evolving

The landscape of financial fraud is undergoing rapid transformation, characterized by a complex interplay of traditional and emerging threats, each presenting unique challenges to FIs. The evolving environment demands constant vigilance and adaptation from defenders as new vulnerabilities emerge alongside innovative financial services and products. FIs find themselves in an ongoing arms race, striving to keep pace ahead of fraudsters who are quick to exploit any weaknesses in the system.

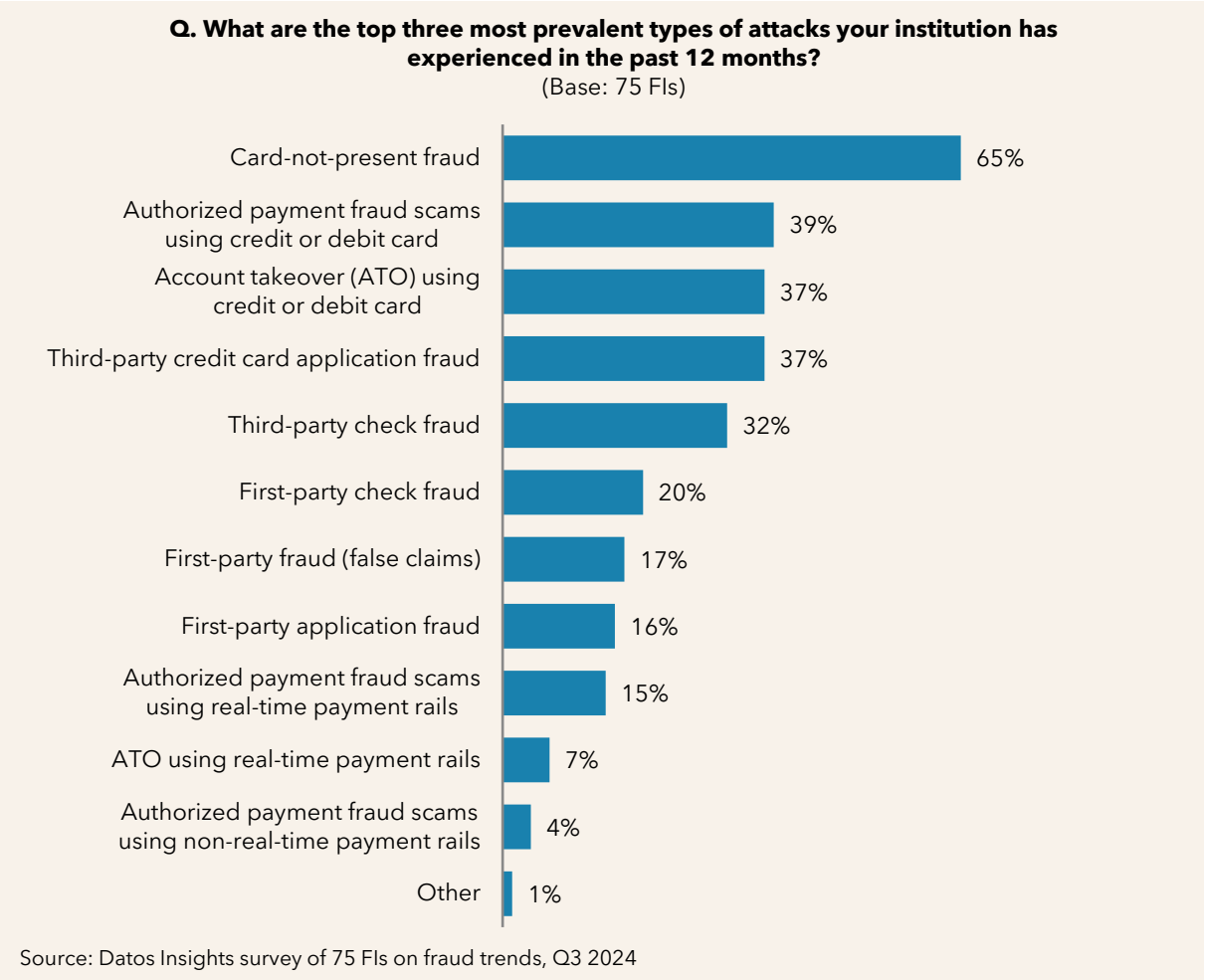
Each fraud type requires a tailored prevention approach, reflecting the multifaceted nature of the current threat landscape. FIs must integrate comprehensive strategies that address established and emerging fraud risks. This necessitates a deep understanding of various fraud methodologies and the ability to rapidly adapt defenses as new threats emerge. Further, an increasing volume of technologically advanced and socially engineered attacks target system vulnerabilities and human behavior.

Looking ahead, the fraud landscape is poised for further evolution, with emerging technologies like AI and machine learning playing dual roles as both threat amplifiers and potential solutions. While these technologies have the potential to create more convincing and scalable fraud schemes, they also offer powerful tools for enhancing fraud detection and prevention capabilities. FIs are increasingly concerned about the potential for these technologies to create more convincing and scalable fraud attacks while simultaneously exploring their use in enhancing fraud detection and prevention capabilities.

Prevalent Attack Types

A wide spectrum of fraud attacks presents unique challenges and risks. Among these varied threats, certain types of fraud have emerged as particularly prevalent and concerning. CNP fraud stands out as the most common attack type, reported by 65% of institutions as a top concern (Figure 1).

Figure 1: Most Prevalent Fraud Attack Types



Source: Datos Insights survey of 75 FIs on fraud trends, Q3 2024

This high prevalence is not surprising given the continued growth of e-commerce and digital transactions, providing an easier target for fraudsters. CNP fraud is particularly attractive to criminals because it doesn't require physical possession of a payment card, making it easier to execute and harder to trace.

Another disturbing trend in fraud is the inclination for FI customers to intentionally engage in fraud or, at a minimum, be tricked by fraudsters into participating in a fraudulent transaction. This is evidenced by the survey findings that authorized payment fraud using real-time payment rails, first-party fraud, false claims, first-party check fraud, and first-party application fraud have emerged as significant issues individually and in the aggregate.

One bank fraud executive interviewed highlighted the alarming prevalence of these types of fraud, stating, "The number of false claims the bank has experienced is shocking. It is really shocking." This trend is so concerning because it changes the dynamic of FIs and

their customers who used to share an aligned self-interest in avoiding fraudulent activity. Further, these trends may suggest a growing willingness of FI customers to get involved in fraud perpetration.

Account takeover (ATO) attacks emerged as another area that has risen to the top of executive concerns. In particular, those ATO attacks that target credit or debit cards were reported by 37% of surveyed institutions as a top concern.

The high incidence of ATO attacks can largely be attributed to the vast amount of personal data and credentials that have been compromised in numerous high-profile data breaches over the past decade. These breaches have flooded the dark web with millions of user-names, passwords, and other sensitive information, providing fraudsters with a treasure trove of resources to fuel their illicit activities. The sheer volume of available data has made it easier for criminals to gain unauthorized access to legitimate accounts, often by exploiting weak or reused passwords.

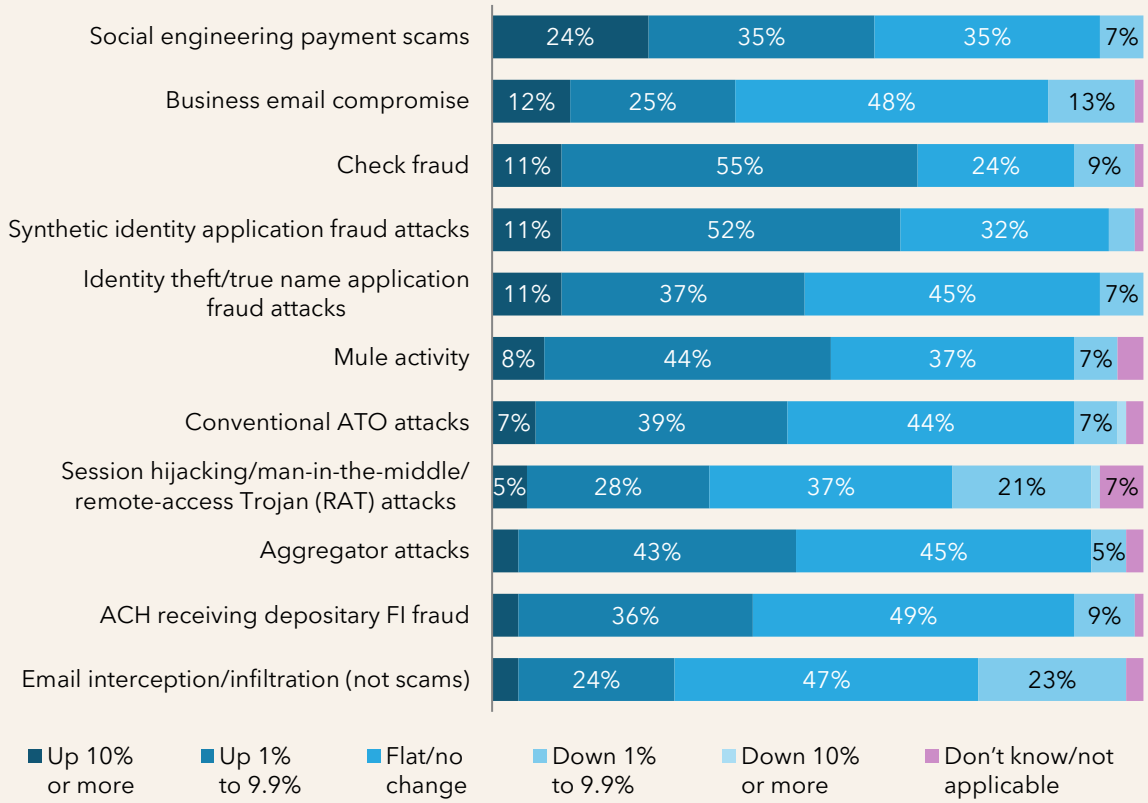
Evolving Fraud Trends

The financial fraud landscape may be undergoing a shift as institutions have witnessed a notable increase in several attack vectors in 2024 compared to 2023. These spikes may highlight the evolving nature of fraud and the ongoing challenges faced by FIs in combating these threats.

Social engineering payment scams, in particular, have experienced a substantial uptick, becoming a major concern for most FIs, with 59% reporting an increase over 2023 (Figure 2).

Figure 2: Evolving Fraud Attack Trends

Q. Please estimate the trend associated with each kind of fraud attack type at your institution, comparing YTD 2024 attack rates to 2023 attack rates.
(Base: 75 FIs)



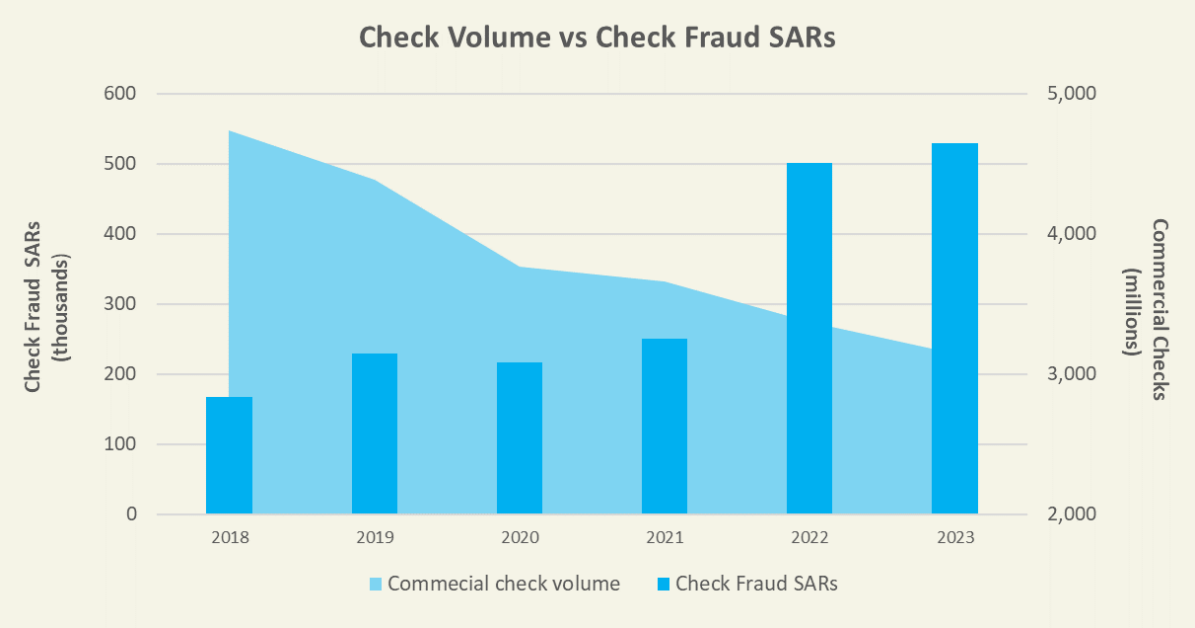
Source: Datos Insights survey of 75 FIs on fraud trends, Q3 2024

Similarly, business email compromise (BEC) has increased as fraudsters focus on large dollar payoffs. This trend underscores the persistent effectiveness of criminals in manipulating unwitting participants. As digital transactions become more commonplace, fraudsters continue to refine their tactics, exploiting human vulnerabilities to bypass technical security measures.

Check Fraud

Check fraud has experienced a resurgence despite the declining use of checks in the U.S. over time. The majority of surveyed FIs report an increase in check fraud activity in 2024 compared to 2023 (Figure 2), and regulatory data further support this trend. As shown in Figure 3, suspicious activity report (SAR) filings involving check fraud more than tripled between 2018 and 2023, even as check volume dropped by 33% over that same period.

Figure 3: Commercial Check Volume and Check Fraud SAR Filings



This increase challenges the assumption that older payment methods are becoming a less attractive vehicle to fraudsters. In fact, it suggests that criminals are opportunistically targeting areas where defenses are vulnerable, particularly those that may have weakened over time due to reduced focus or a lack of ongoing investment. One bank executive provided insight into their institution's experience with check fraud, stating: "Check fraud has been up between one and 10%. My firm has had less check fraud than what has been heard and read about in the industry, but we were hit hard in July by a treasury check attack."

Synthetic Identity Fraud

Synthetic identity fraud attacks have also risen significantly, with 63% of institutions reporting an increase. This reflects the growing sophistication of fraudsters in creating and nurturing fake identities that can bypass traditional identity verification methods. Concurrently, fraud-fighting professionals are becoming increasingly concerned about fraudster's potential exploitation of GenAI in creating more realistic identities and curating those identities over time to generate even larger fraud payoffs due to line increases and other cross-selling processes.

Money Mules

The influx of money mules is concerning fraud executives. Mule activity has surged, with 52% of institutions reporting increases as fraudsters move funds from various scams and

other predicate crimes (Figure 2). Meanwhile, regulatory pressures are building globally. Regulators in various jurisdictions, such as the U.K., are signaling a move to a new model of shared liability between sending and receiving FIs. This marks a shift from the current system, where sending banks bear the full burden of losses. Other jurisdictions, such as the U.S., may follow suit. This regulatory pressure may propel receiving banks to better screen inbound payments and push the industry to engage in more targeted data sharing in relation to bad recipients.

Prospective Fraud Concerns

FIs are particularly worried about several emerging fraud threats, with the impact of AI amplifying these. Synthetic identities resulting from application fraud top the list of concerns for the next two years, with 56% of institutions identifying this as a major imminent risk, as shown in Figure 4.

Figure 4: Prospective Fraud Threats

Q. Considering your institution's control framework's ability to detect attacks/ prevent losses, which three fraud types concern you most in the next two years?
(Base: 75 FIs)

Source: Datos Insights survey of 75 FIs on fraud trends, Q3 2024

The sophistication of synthetic identities is expected to increase due to the introduction of GenAI. One fraud executive interviewed noted, "If I were using AI to do something, I would use it to dig through lots of stolen data and build that out because so much data is compromised." This indicates a general foreboding that AI could significantly enhance the creation of more convincing synthetic identities at a greater scale by efficiently processing and combining vast amounts of stolen personal data.

ID theft and true name fraud resulting from application fraud are other significant concerns cited by 36% of institutions. The availability of compromised data makes this threat vector particularly concerning. As one bank executive noted, "The ability to verify identities digitally is the lifeblood of a bank, so that is a big risk, just in terms of the weight on it from a criticality perspective."

ATO attacks, particularly those targeting wire transfers at 31%, peer-to-peer (P2P) transactions at 21%, and cards at 20%, are expected to remain a major threat as FIs continue the ongoing fight to secure customer accounts and data. In the words of one bank executive interviewed: "ATO has definitely increased. It is one of my firm's hotter areas, especially during the third quarter of 2024. Right now, this is top of mind." The integration of AI in ATO attacks could also lead to more nuanced and harder-to-detect account compromises, as the technology could learn and mimic legitimate user behaviors more accurately.

AI in Fraud: Perpetration and Prevention

The advancement of AI is influencing fraud perpetration and prevention in the financial sector. As FIs work to improve their defenses, fraudsters are adopting these tools to enhance their methods. This technological development is changing the fraud landscape, creating new challenges while providing opportunities for improved detection and prevention.

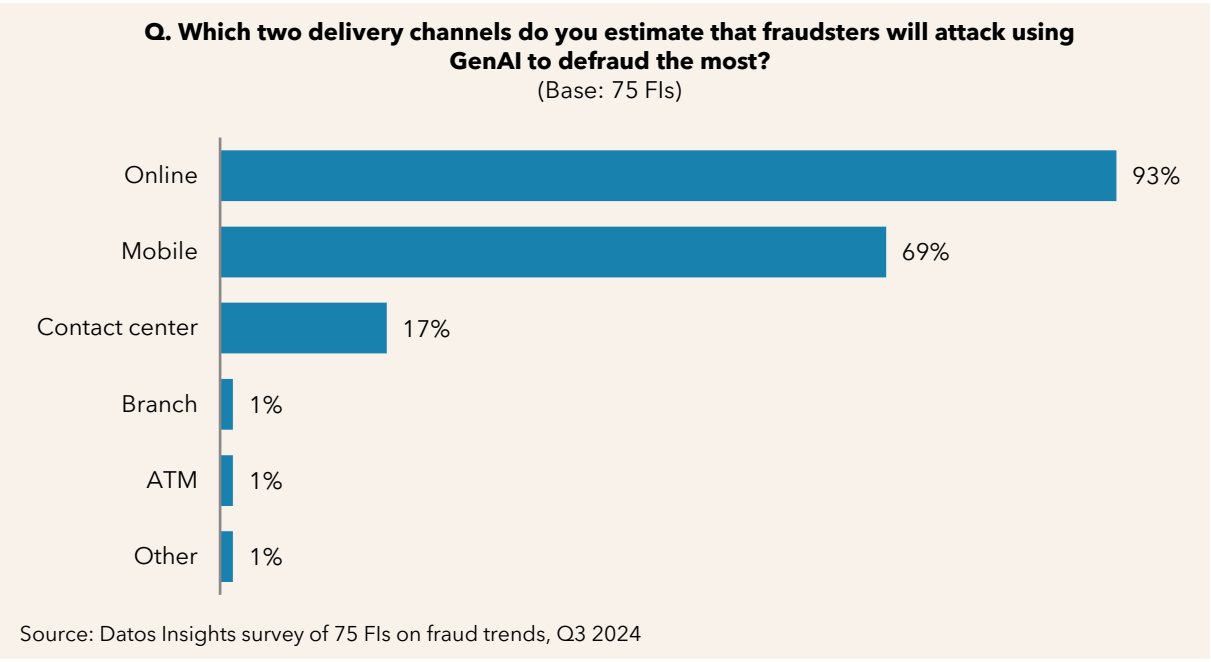
FIs face regulatory hurdles when implementing AI solutions, a factor that criminals are able to disregard. The potential for bias, lack of explainability in AI models, and data privacy issues are just a few of the concerns that worry regulators and drive new legislation and guidance to protect society from the potential misuse of AI. For instance, in the U.S., the Federal Reserve's guidance on model risk management (SR 11-7) requires banks to demonstrate understanding and control over their models, including AI-based ones.[1]

Additionally, the U.S. Consumer Financial Protection Bureau (CFPB) has indicated increased scrutiny of AI use in financial services, particularly regarding fair lending practices. These regulatory considerations necessitate a cautious approach to AI adoption in fraud prevention.

The apprehension among fraud executives is evident, with 93% of surveyed FIs expressing alarm about defending against AI-powered attacks in the online channel and 69% indicating similar worries about the mobile channel (Figure 5). At the same time, many institutions are exploring AI's potential to strengthen their fraud prevention capabilities, albeit within regulatory constraints.

[1] "SR 11-7: Guidance on Model Risk Management," Federal Reserve, April 4, 2011, accessed October 23, 2024, https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm#:~:text=The%20Federal%20Reserve%20and%20Office,governance%2C%20policies%2C%20and%20controls.

Figure 5: GenAI Attacks by Delivery Channel



Source: Datos Insights survey of 75 FIs on fraud trends, Q3 2024

One bank fraud executive noted, "Our fraud organization is likely to use AI if model governance and explainability are met," highlighting the importance of factoring in and achieving regulatory compliance in AI adoption. This emphasizes the complex interplay that institutions must balance between technological advancement, regulatory compliance, and financial security in the current digital environment, particularly while fraudsters are unfettered in their use of the technology.

Attack Vectors

AI has powered fraudsters to expand their arsenals and refine their attack capabilities. Machine learning algorithms allow for more sophisticated data analysis, enabling criminals to identify and exploit vulnerabilities with greater precision. Natural language processing and generation technologies have elevated social engineering tactics, making phishing attempts and impersonation scams increasingly difficult to detect and more effective in fooling consumers and businesses.

Perhaps most concerning is AI's potential to automate and scale traditionally labor-intensive fraudulent activities. With the ability to generate countless variations of attack strategies and test them in real time, AI empowers fraudsters to evolve their tactics at an unprecedented pace. This rapid evolution presents a significant challenge, as traditional fraud detection models may struggle to keep up with the ever-changing landscape of

AI-driven attacks. Fraud prevention experts have identified several key areas in which AI has the potential to enhance fraudsters' capabilities, as shown in Table A.

Table A: Fraudster Use of GenAI and Deepfake Technology

Fraudulent use case	Description
Creating synthetic identities	AI algorithms can generate complex, realistic synthetic identities by combining elements from multiple stolen identities and fabricated information.
Fueling social engineering	AI-powered chatbots and voice synthesis technologies are making social engineering attacks more sophisticated and believable. These AI tools can mimic human conversation patterns and even replicate known voices, making it easier for fraudsters to manipulate victims at a greater scale.
Circumventing biometric authentication	Deepfake technology poses a significant threat to voice and video-based authentication methods. AI-generated deepfakes can potentially bypass biometric security measures, undermining the reliability of advanced authentication techniques, and fool relatives by mimicking voice or video.
Scaling attacks through automation	AI enables fraudsters to automate their attacks on a massive scale. This capability allows fraudsters to target multiple institutions simultaneously and quickly adapt their tactics based on success rates, making it challenging for FIs to keep pace with evolving threats.

Source: Datos Insights

The democratization of AI tools means that sophisticated attack methods, previously limited to well-resourced criminal organizations, are now more accessible to a broader range of bad actors, potentially leading to a surge in both the volume and sophistication of fraud attempts.

Fraud executives expressed a general sentiment of caution regarding AI-powered attacks. As one bank fraud executive summarized, "AI-powered attacks may be manageable in the next two years, but they will exceed the improved defenses." This perspective demonstrates the ongoing challenge FIs face in developing effective countermeasures against AI-enhanced fraud tactics.

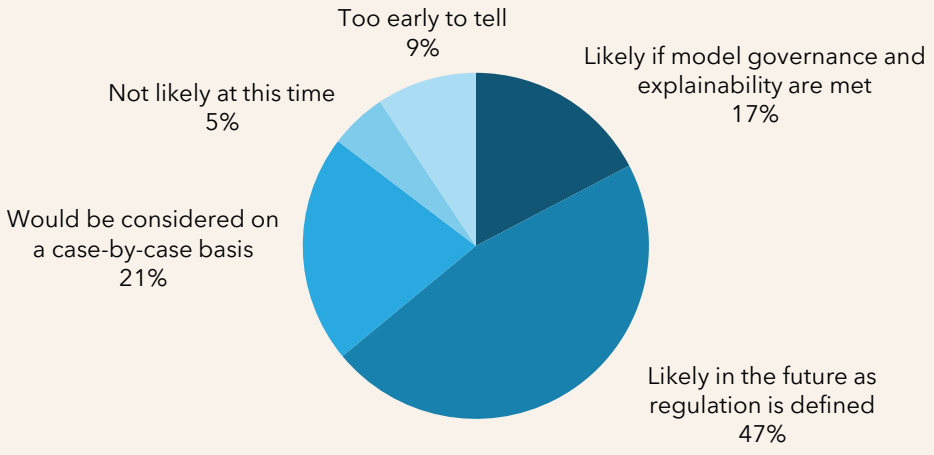
Defense Mechanisms

AI presents formidable challenges in fraud prevention, but it also offers powerful tools for FIs to bolster their defenses. The key lies in leveraging AI's capabilities to create more dynamic, adaptive, and intelligent fraud detection systems. By harnessing the power of machine learning and big data analytics, institutions can develop fraud prevention strategies that evolve in real time, keeping pace with increasingly sophisticated fraud attempts. However, the implementation of AI in fraud prevention is not without its challenges. Concerns about model explainability, data privacy, and the potential for algorithmic bias must be carefully addressed.

Despite challenges, FIs are cautiously optimistic about AI's potential role in fraud prevention. A plurality of fraud executives (47%) expect that GenAI is likely to be used to detect fraud as regulations are defined; an additional 17% believe it will if model governance and explainability requirements are met (Figure 6).

Figure 6: GenAI Use in Fraud Detection

Q. How likely is your institution to allow for the use of GenAI to detect fraud at this time?
(Base: 75 FIs)



Source: Datos Insights Survey of 75 FIs on Fraud Trends, Q3 2024

As one bank executive stated, "We view it through the lens of whether we can use transformer-type approaches to make our existing models a lot better." This sentiment reflects a measured approach to AI integration, focusing on enhancing existing systems rather than wholesale replacement.

FIs are actively exploring AI-powered defense mechanisms, with a primary focus on real-time authentication systems and anomalous pattern detection. These advanced systems are designed to identify and respond to suspicious activities as they occur rather than relying on post-transaction analysis. Table B identifies key use cases being explored by FIs and solution providers. These use cases are particularly critical for strengthening authentication processes and detecting unusual patterns that may indicate fraudulent behavior.

Table B: Fraud Prevention Use of GenAI Technology

Beneficial use case	Description
Enhanced anomaly detection	AI models can analyze vast amounts of transaction data to identify suspicious patterns more accurately and quickly than traditional rule-based systems. These models can continuously learn and adapt to new fraud patterns, improving their detection capabilities over time.
Behavioral biometrics	AI-powered behavioral analysis can help distinguish between legitimate users and fraudsters based on subtle patterns in how they interact with devices and applications. This technology can detect nuances such as typing speed, mouse movements, and touchscreen pressure, creating a unique "behavioral fingerprint" for each user.
Real-time fraud scoring	Machine learning models can provide real-time risk scores for transactions, allowing for more nuanced and accurate fraud detection. These scores can be integrated into existing fraud prevention workflows, enabling FIs to make split-second decisions on whether to approve, deny, or flag a transaction for further review.
Adaptive authentication	AI can help create dynamic authentication processes that adjust based on the risk level of each transaction or interaction. This approach allows for a seamless user experience in low-risk scenarios while implementing stronger security measures when potential threats are detected.
Synthetic identity detection	Advanced machine learning models are being developed to identify synthetic identities by analyzing patterns and inconsistencies in application data. These models can cross-reference multiple data sources and identify subtle discrepancies that might indicate a fabricated identity, even when the individual pieces of information appear legitimate.

Source: Datos Insights

Defending Your Institution: Key Investment Areas

FIs are strategically allocating resources to strengthen their defenses, with a clear focus on technologies and processes that address current and emerging fraud threats. These investments reflect holistic approaches to fraud prevention, encompassing identity verification, transaction monitoring, and advanced analytics. The prioritization of these areas demonstrates a growing recognition that effective fraud prevention requires a multilayer strategy that can adapt quickly.

Several factors—such as the prevalence of specific fraud types, the potential impact of emerging technologies, and the need to balance fraud detection with customer experience—are driving the focus on key investment areas. Fraud executives recognize the need for short-, medium- and long-term strategies. Short-term investments focus on immediate threat mitigation; longer-term strategies involve more substantial changes, typically requiring system development or vendor integrations. A majority of fraud executives (56%) would prefer to address new fraud threats through a more considered process that seeks to fill a gap through purpose-built solutions (Figure 7).

Figure 7: Addressing Fraud Trends Through Investment

Source: Datos Insights survey of 75 FIs on fraud trends, Q3 2024

However, there is also a realization that time is money when it comes to fraud losses, and they often have to work faster through the leveraging of available tools.

One fraud executive highlighted the importance of rapid implementation in an investment strategy: "From a practical perspective, six months is the minimum viable amount of time." This fraud executive also noted the value of leveraging existing vendor relationships for quicker deployment of new solutions. "We've moved more towards taking that approach of trying to pursue strategic relationships where we have the ability to extend an existing association so that in a crisis, we don't find ourselves caught without an option."

While FIs are focusing on technological solutions and enhancing their operational capabilities to respond more quickly and effectively to new fraud threats, they recognize that sometimes that preferred path is not available. As one executive put it, "We will ramp up our operational expense by reviewing everything, or we will degrade the customer experience if we have to." This approach exemplifies the balance between immediate action and long-term strategic investments in fraud prevention and the potential impact on customer experience.

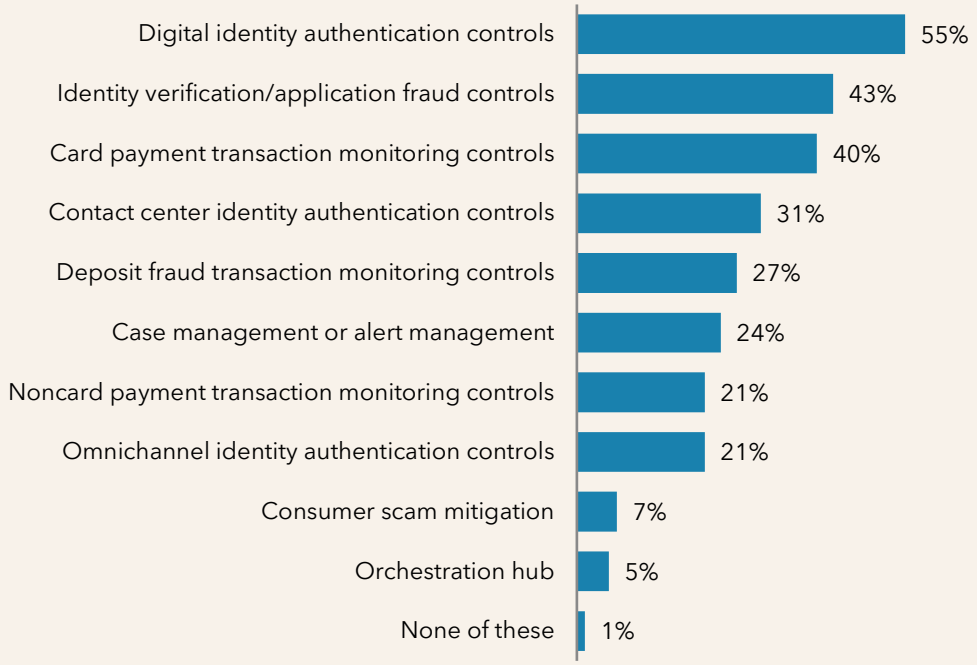
Trends in Fraud Prevention Investments

Datos Insights' research highlights several key investment priorities that are shaping the future of fraud prevention in the financial services industry. Investments reflect a proactive approach to addressing both current pain points and anticipated future challenges. By strategically allocating resources to these areas, FIs are not only bolstering their immediate defenses but also laying the groundwork for more resilient and adaptable fraud prevention ecosystems in the long term.

Digital identity authentication and verification emerge as top priorities: 55% of institutions identify them as a key investment area. Identity verification controls placed second, with 43% of executives indicating transformation plans in this area (Figure 8).

Figure 8: Fraud Investment/Transformation Areas

Q. At your institution, which three areas are getting the most funding in terms of investment/transformation?
(Base: 75 FIs)



Source: Datos Insights survey of 75 fls on fraud trends, Q3 2024

This focus on identity verification reflects its fundamental importance in fraud prevention, particularly in combating ATO and synthetic identity fraud. Fraud executives have expressed serious concerns about their current identity verification capabilities, as these tools may not be keeping pace with evolving threats. The success rate of fraudsters in circumventing existing controls underscores the urgent need for more robust verification solutions.

The emphasis on identity-related investments is closely followed by a need to enhance transaction monitoring capabilities. Card payment fraud prevention, in particular, has emerged as a critical focus area, with 40% of institutions planning significant investments in this space. This emphasis on card payment monitoring reflects the continued prevalence of card-not-present fraud, which remains one of the most significant threats facing financial institutions today.

Other areas receiving investment attention include the following:

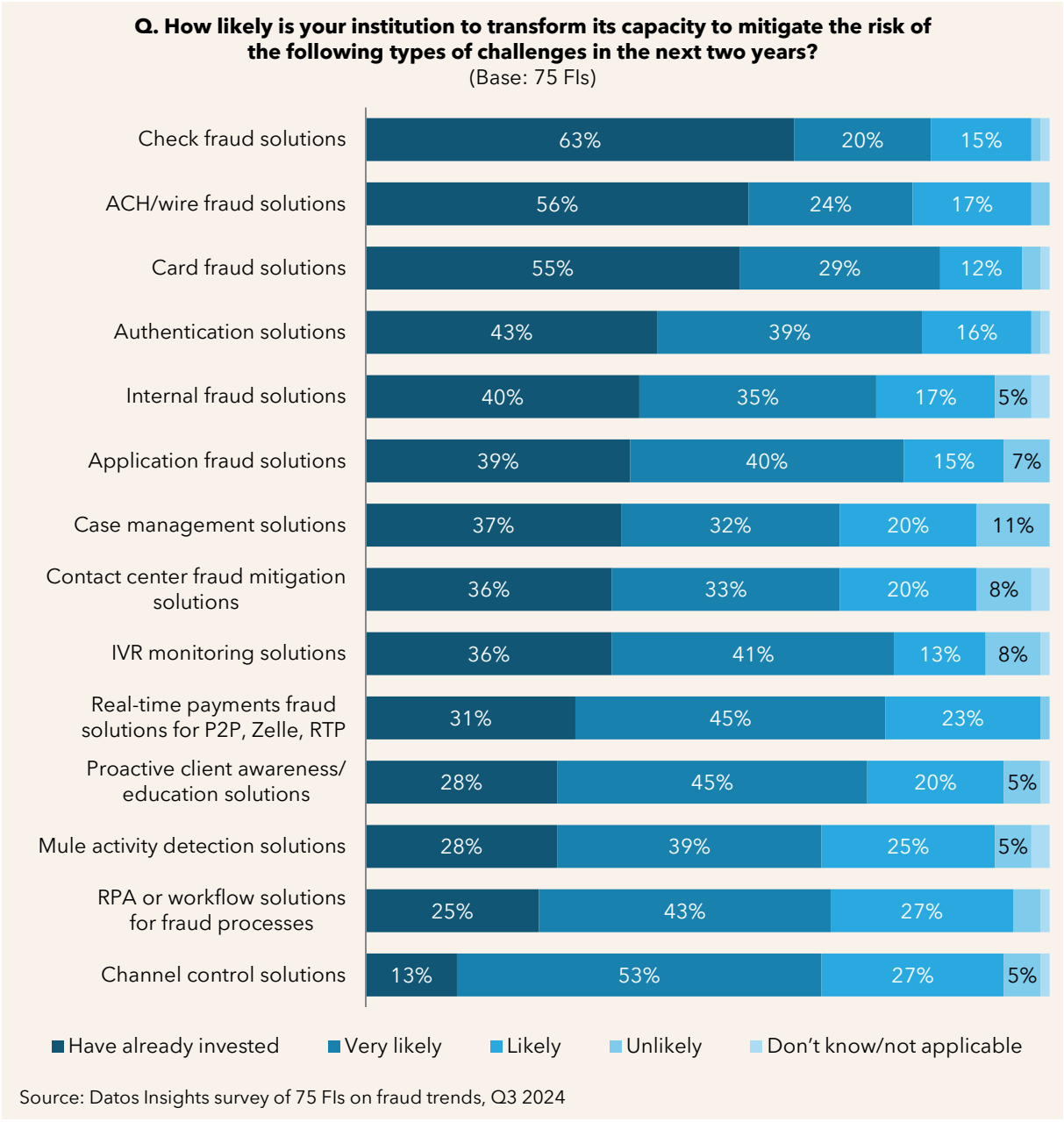
- **Contact center authentication controls:** It is generally recognized that a sizable percentage of fraud committed against FIs is in part related to information that is socially engineered through the contact center. Consequently, it's not surprising that 31% of FIs are looking to improve authentication controls in that area, especially in light of the enhanced threat related to AI.
- **Case management and alert management:** As institutions look to improve operating expenses, they are also looking to enhance their case and alert management capabilities. Nearly one-fourth of fraud executives (24%) indicated that they were seeking to streamline their fraud response processes and improve operational efficiency.
- **Consumer scam mitigation:** With the rise in sophisticated scams, it is surprising that so few institutions (7%) indicated that they have invested in education and detection capabilities to protect their customers from being duped into sending money to fraudsters.

Skating to the Puck: Investing Ahead

Forward-thinking FIs are not only addressing current fraud challenges but also positioning themselves to tackle emerging threats. This proactive approach involves investing in technologies and capabilities that may not yet be fully mature but show promise in addressing future fraud scenarios. By staying ahead of the curve and exploring innovative solutions, FIs are seeking to build a foundation of adaptability and resilience that will be crucial in navigating the increasingly complex and dynamic fraud landscape of tomorrow.

The rapid evolution of payment technologies, particularly in the realm of real-time payments, is driving significant investment in fraud prevention solutions tailored to these new channels. Real-time payments are among the most common focus areas for fraud investment. A resounding 99% of FIs have either invested in or are likely to invest in fraud solutions specifically designed for faster payment systems (Figure 9).

Figure 9: Prospective Investments in Fraud Transformation



Source: Datos Insights survey of 75 FIs on fraud trends, Q3 2024

This near-universal commitment to enhancing fraud prevention in the real-time payment ecosystem underscores the critical importance of safeguarding this rapidly expanding channel. FIs recognize that the speed and convenience of instant transactions must be balanced with robust security measures to maintain customer trust and mitigate potential losses.

Synthetic identity fraud and other forms of application fraud are also likely to attract investment in more sophisticated application fraud solutions. A striking 55% of institutions reported that they are planning on investing in this area, while 39% indicated that they had already made progress, highlighting the industry's recognition of the long-term threat posed by these fraud types. This widespread focus on combating application fraud reflects an understanding among FIs that traditional identity verification methods are increasingly inadequate in the face of highly sophisticated synthetic identities, necessitating more advanced, multilayer approaches to detect and prevent these evolving threats.

Institutions are also focusing on other key areas of forward-looking investments in fraud detection:

- **Authentication solutions:** Advanced authentication technologies have seen significant investment, with 82% of fraud executives having already invested or very likely to invest in these solutions. This high level of investment reflects the critical role of robust authentication in preventing ATO and other fraud types.
- **Mule activity detection:** Several bank fraud executives interviewed highlighted mule detection as an emerging investment area, recognizing the pivotal role of mule accounts in facilitating various fraud schemes and concerns over sharing of related liability.
- **AI and machine learning capabilities:** While approached cautiously, FIs are exploring AI investments to enhance their fraud detection and prevention capabilities, particularly in areas like synthetic voice detection and document verification.
- **Vendor relationship management:** Many institutions are prioritizing the ability to quickly implement new solutions, particularly through existing vendor relationships, allowing for more agile responses to emerging threats.

As FIs continue to invest in new fraud prevention technologies, they are positioning themselves at the forefront of the ongoing battle against financial crime. This proactive stance not only protects their assets and customers in the present but also builds a foundation for future resilience in an increasingly complex digital landscape. By embracing innovation and staying ahead of emerging threats, these institutions are not just defending against fraud; rather, they are actively shaping the future of financial security.

Conclusion

The landscape of financial fraud is evolving at an unprecedented pace, driven by technological advancements and the increasing sophistication of fraudsters. As FIs navigate this complex terrain, they must adopt a proactive and adaptive approach to fraud prevention that balances immediate threat mitigation with long-term strategic investments. To effectively approach fraud investments in the current environment, FIs should consider the following recommendations:

- **Prioritize digital identity authentication and verification:** With synthetic identity fraud and ATO attacks on the rise, robust identity verification is crucial. Invest in advanced technologies that can detect sophisticated fraudulent identities and authenticate legitimate users accurately.
- **Enhance real-time payment fraud solutions:** As faster payment systems become more prevalent, ensure that fraud detection capabilities can keep pace. Invest in solutions that can analyze transactions and detect anomalies in real time.
- **Develop a comprehensive AI strategy:** While being mindful of regulatory constraints, explore AI and machine learning capabilities to enhance fraud detection and prevention. Focus on areas like anomaly detection, behavioral biometrics, and adaptive authentication.
- **Strengthen contact center authentication:** Recognize the vulnerability of contact centers to social engineering attacks. Implement advanced voice authentication technologies and train staff to identify potential fraud attempts.
- **Improve case management and alert systems:** Streamline fraud response processes to improve operational efficiency and reduce false positives, allowing for quicker and more accurate fraud detection.
- **Foster agile vendor relationships:** Cultivate partnerships with fraud prevention vendors that allow for quick implementation of innovative solutions, enabling more rapid responses to emerging threats.

As the fraud landscape continues to evolve, FIs must remain vigilant and adaptable in their approach to fraud prevention. By implementing these recommendations and staying abreast of emerging threats, institutions can build a resilient fraud prevention ecosystem that protects both their assets and their customers in an increasingly digital world.

About Early Warning Services

Early Warning Services, LLC, a financial services technology leader, has been empowering and protecting consumers, small businesses, and the U.S. financial services ecosystem with cutting-edge fraud and payment solutions for more than three decades. Through unmatched network intelligence and partnerships with more than 2,500 bank and credit union brands, we increase access to financial services and products and protect financial transactions. We are the company behind Zelle and Paze, an online checkout solution. To learn more, visit www.earlywarning.com.

About Datos Insights

Datos Insights is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

Contact

Research, consulting, and events:

sales@datos-insights.com

Press inquiries:

pr@datos-insights.com

All other inquiries:

info@datos-insights.com

Global headquarters:

6 Liberty Square #2779
Boston, MA 02109

www.datos-insights.com

Author information

Jim Mortensen

jmortensen@datos-insights.com

David Barnhardt

dbarnhardt@datos-insights.com