March 2025

Advancing Fraud Prevention: Orchestration Solution Adoption in Financial Services

David Barnhardt and Jim Mortensen

This report provided compliments of:

March 2025

Advancing Fraud Prevention: Orchestration Solution Adoption in Financial Services

David Barnhardt and Jim Mortensen

Table of Contents

List of Figures

List of Tables

Summary and Key Findings

Fraud orchestration solutions have emerged as a promising option for financial institutions seeking to modernize fraud prevention capabilities while maintaining operational efficiency and customer satisfaction. Using these systems, FIs can coordinate multiple fraud-detection systems, data sources, and authentication tools while providing real-time decision-making capabilities across channels.

This report examines current issues, technology adoption patterns, and emerging fraud prevention and orchestration priorities. It also recommends ways organizations should embark on the orchestration journey to avoid becoming increasingly vulnerable to changing fraud patterns and losing consumer trust. It is based on interviews conducted with 19 FI fraud prevention executives between November and December 2024.

The following are key findings from this report:

- **Data silos and integration complexity are primary obstacles in fraud prevention.** The inability to effectively consolidate and analyze data across systems creates significant vulnerabilities within FIs that sophisticated fraudsters increasingly exploit.
- **Real-time fraud-detection capabilities remain inadequate across the industry.** As payment speeds increase and customer expectations for immediate transactions grow, FIs must find new, more accurate ways to detect fraud. The need to integrate multiple data sources and apply sophisticated analytics within milliseconds creates significant challenges that many institutions struggle to address.
- **Most institutions are investing in technology to address fraud prevention hurdles while also implementing stop-gap measures.** Many organizations find themselves balancing immediate tactical needs with longer-term strategic investments, often implementing manual workarounds.
- **Fraud orchestration solutions show strong adoption momentum, and emerging technologies are garnering interest.** Most institutions are taking a targeted, phased approach to implementing these systems, focusing initially on specific high-priority areas instead of attempting comprehensive coverage. There is also strong interest in artificial intelligence (AI)-powered anomaly detection and behavioral biometrics.

- **The research reveals a clear industry trajectory toward more sophisticated, integrated fraud prevention approaches driven by the need to address increasingly complex threats while maintaining operational efficiency.** FIs must balance immediate tactical needs with strategic technology investments as they work to orchestrate and modernize their fraud prevention ecosystem.

Introduction

As digital transformation accelerates and customer expectations for real-time services grow, the financial services industry faces unprecedented fraud prevention challenges. Fraudsters increasingly exploit the gaps between traditional controls and modern banking channels, using sophisticated techniques that combine social engineering, synthetic identities, and automated attacks. The increasing speed of payments and growing variety of digital touch points create new vulnerabilities that traditional fraud prevention approaches struggle to address.

FIs are caught between the need to provide seamless customer experiences with minimal friction and the imperative to prevent increasingly sophisticated fraud attacks. Many institutions resort to adding staff and implementing additional manual processes to compensate for identified technology gaps. Fraud orchestration solutions have emerged as a promising alternative to these tactics. They offer FIs the ability to coordinate multiple fraud-detection systems, data sources, and authentication tools while providing real-time decision-making capabilities across channels. By providing a centralized platform for managing fraud prevention across channels and systems, orchestration solutions help institutions address the fundamental issues of siloed data and the need to be more responsive.

FIs that have deployed these capabilities report significant benefits, including improved fraud-detection rates and enhanced customer experience. While the implementation journey often proves complex, FIs that do not embrace orchestration will find themselves increasingly vulnerable to changing fraud patterns and lost consumer trust. This report examines fraud orchestration solutions for FIs to help inform their technology selection process while highlighting key considerations for implementation.

Methodology

This report draws upon interviews conducted with 19 FI fraud prevention executives between November and December 2024. The participating organizations represent a diverse cross-section of the industry, including large national banks (11), regional banks (six), and credit unions (two) with greater than US$10 billion in assets. Interviewees hold senior positions in fraud prevention, financial crimes, and risk management. The research focused on understanding current fraud prevention barriers, orchestration solution adoption patterns, and emerging technology priorities.

Fraud Solutions Market Landscape

FIs are grappling with a surge in fraudulent activities across traditional and emerging payment channels, forcing them to reevaluate their approaches to fraud detection and prevention. Several market forces are driving FIs to seek more sophisticated, integrated solutions that can effectively address conventional fraud schemes and new attack vectors emerging in the digital age (Table A).

Table A: Market Forces Impacting Fraud Prevention Technology Needs

Market force	Impact
Digital acceleration	Digital channels often lack sufficient controls, and FIs are struggling to assess high-risk transactions, especially in scenarios involving peer-to-peer (P2P) or bill-pay systems. As customers increasingly favor mobile and online transactions, organizations must leverage device-specific data and digital behavioral patterns to enhance fraud-detection capabilities while maintaining a more seamless customer experience across channels.
Data silo barriers	Organizations struggle to consolidate internal data sets residing across products and channels due to inconsistent formats and quality standards. This fragmentation creates significant barriers when attempting to construct unified customer profiles for fraud-detection purposes.
External data access	FIs need greater access to data sets that provide greater visibility of their customers' behaviors. Consortium data access is key to effective fraud prevention.
Evolving fraud threats and growing sophistication	Modern fraudsters employ increasingly advanced tools and techniques, necessitating enhanced detection capabilities. In response, organizations must expand their end-to-end monitoring of risk signals and strengthen verification methods to effectively counter evolving threats. This evolution is driving demand for more advanced authentication methods and the ability to orchestrate multiple risk signals across various platforms.

Market force	Impact
Resource utilization	Under the constant pressure to do more with less, FIs must maximize fraud prevention effectiveness while reducing vendor relationships, technology costs, and human resources. Banks need ways to automate workflows and reduce manual intervention, particularly for lower-risk transactions. This resource constraint is pushing organizations toward consolidated platforms that can replace several point solutions while improving operational efficiency.
Analytic advancements	Advancements in AI and machine learning (ML) technologies have transformed the landscape of fraud prevention, making sophisticated analytical capabilities more accessible and cost-effective than ever before. These functions are becoming table stakes, and FIs are looking for platforms that can harness these technologies and identify subtle patterns that might indicate fraudulent activity. FIs of all sizes are implementing solutions that leverage ML algorithms to continuously improve fraud-detection accuracy while automating decision workflows.

Source: Datos Insights

These market forces reflect the complex landscape of fraud prevention facing FIs today. An array of interconnected issues—from digital channel vulnerabilities to data silos and resource constraints—are driving organizations toward comprehensive orchestration solutions that can integrate diverse data sources and analytical capabilities. As fraud schemes grow more sophisticated and digital transactions increase, institutions require platforms that not only consolidate their fraud prevention efforts but also leverage advanced AI and ML technologies to identify emerging threats. The ability to break down data silos, incorporate external intelligence, and automate workflows has become essential for maintaining effective fraud prevention while optimizing resources and preserving the customer experience.

Current FI Fraud Defenses

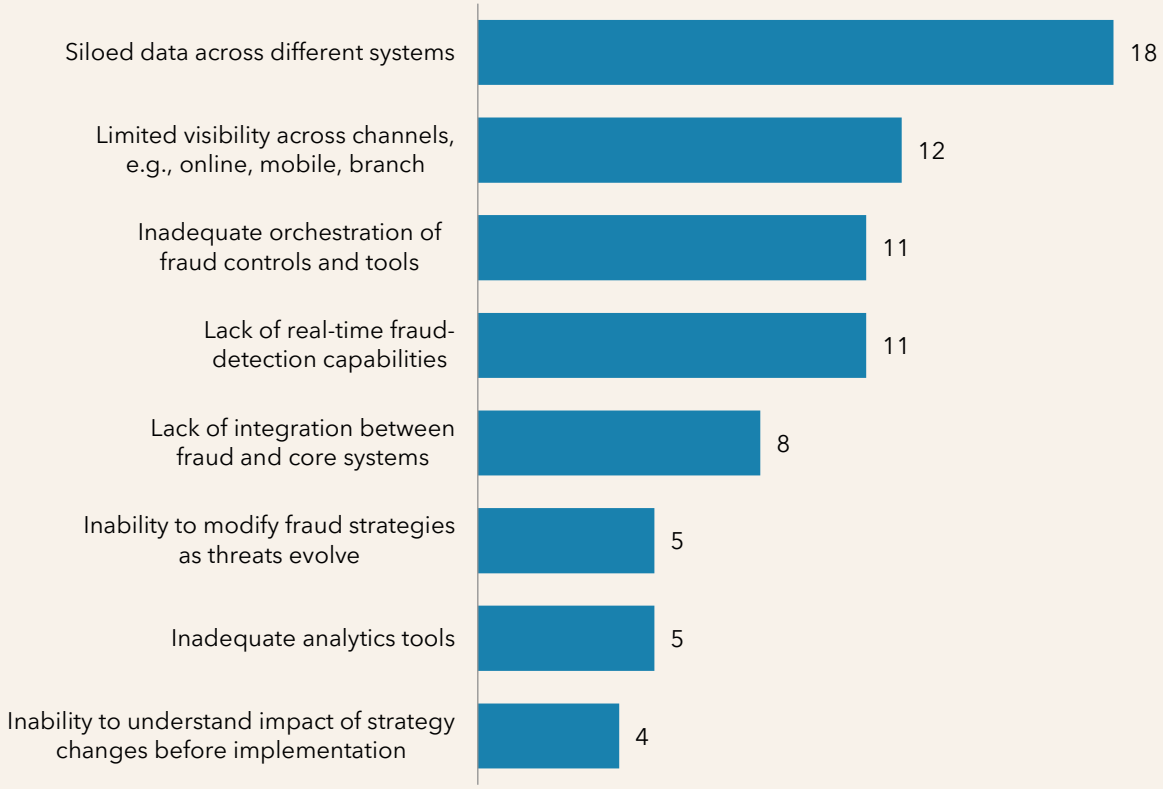
Most institutional fraud prevention capabilities reflect years of layering point solutions and specialized tools onto legacy infrastructure, creating complex and often fragmented defense frameworks. Many organizations operate with multiple core systems, payment platforms, and digital channels that do not effectively share information, creating dangerous blind spots between these siloed environments.

The resulting technical limitations force many FIs to implement costly workarounds, such as working from offline exception lists, to compensate for technology gaps. Meanwhile, fraudsters actively exploit the seams between these disconnected systems. This fragmented approach not only increases operational costs but also creates systemic vulnerabilities that sophisticated criminals increasingly identify and target, moving among siloed systems to avoid detection.

Technical Barriers in Fraud Prevention

Integration complexity stands out as the primary obstacle FIs face when implementing modern fraud solutions, particularly when dealing with internal data sources. Of the 19 surveyed FIs, 18 (95%) indicated that siloed data is their primary problem (Figure 1). Siloed data creates significant barriers to effective fraud prevention, as critical customer information remains trapped in disparate systems that cannot easily communicate with one another.

Figure 1: Primary Technology Challenges in Combating Fraud



Source: Datos Insights interviews with 19 U.S. FIs, Q4 2024

FIs rated cross-channel visibility as the second biggest issue, reflecting the heightened importance of unimpeded data views. Without a comprehensive view of customer activities across mobile, online, branch, and call center channels, FIs miss important contextual signals, such as multiple customer contacts across channels at odd hours, that help distinguish legitimate behavior from fraudulent attempts.

The complexity is further compounded when institutions attempt to integrate external data sources and third-party risk signals into their existing fraud prevention framework. While these additional data points can dramatically improve detection capabilities, they often require significant resources to implement and maintain properly.

Moreover, the rise in real-time payment transactions has amplified these challenges by introducing the element of time. Real-time payments demand split-second decisions with limited data. Most institutions operate in a hybrid environment wherein some products

process in real time while others require 'day-two processing,' creating inconsistencies in fraud-detection capabilities. This requires tailored strategies that consider the speed of the transaction, the channel in which it was initiated, and the ability to leverage all relevant data in the risk assessment.

Data Silos and Integration Challenges

Fragmented data environments impede effective fraud prevention. Many organizations have multiple core systems, payment platforms, and digital channels that don't effectively share information. Fraud prevention leaders struggle with integrating new fraud prevention tools into their existing technology stack, particularly when dealing with legacy core banking systems. The challenge extends beyond simple technical integration, as institutions must also navigate complex data governance requirements and ensure consistent data quality across systems.

The impact of data silos becomes particularly acute when FIs attempt to implement real-time fraud prevention capabilities. Executives report that accessing and analyzing data from multiple systems in real time presents significant technical challenges. One fraud leader described his institution as a "Frankenbank" due to the complexity of their system landscape, highlighting the difficulties many organizations face in achieving a unified view of customer activity and risk.

Cross-Channel Visibility Issues

Many FIs struggle to maintain consistent visibility across different channels and customer touch points. The proliferation of digital channels, combined with traditional branch and contact center interactions, creates complex monitoring challenges that many existing systems weren't designed to handle. FIs report that attacks are not focused on a single channel, and the inability to correlate customer activities across channels creates vulnerabilities that sophisticated fraudsters increasingly exploit.

The push for omnichannel banking services further complicates the cross-channel visibility issue. Fraud prevention leaders report difficulties in maintaining consistent fraud controls across channels while delivering the seamless experience customers expect. Many FIs find that their channel-specific fraud prevention tools create inconsistent customer experiences and leave gaps that fraudsters can exploit. Coordinating fraud prevention across channels while maintaining consistent customer experience is a critical capability for many organizations based upon management imperatives.

Real-Time Detection Capabilities

Many FIs believe their real-time detection capabilities are inadequate (as indicated by 58% of FIs in Figure 1), especially as payment speeds increase and customer expectations for immediate transactions grow. Real-time detection becomes more complex as institutions attempt to balance security with customer experience.

Fraud prevention leaders report particular difficulty in maintaining consistent response times while performing comprehensive fraud risk assessments. Integrating multiple data sources and applying sophisticated analytics within milliseconds creates significant technical challenges.

Analytics Gaps

Some institutions still rely heavily on rules-based systems, limiting their ability to detect and respond to emerging fraud patterns effectively. The lack of sophisticated analytics tools, combined with orchestration issues, creates challenges in adapting to new fraud patterns.

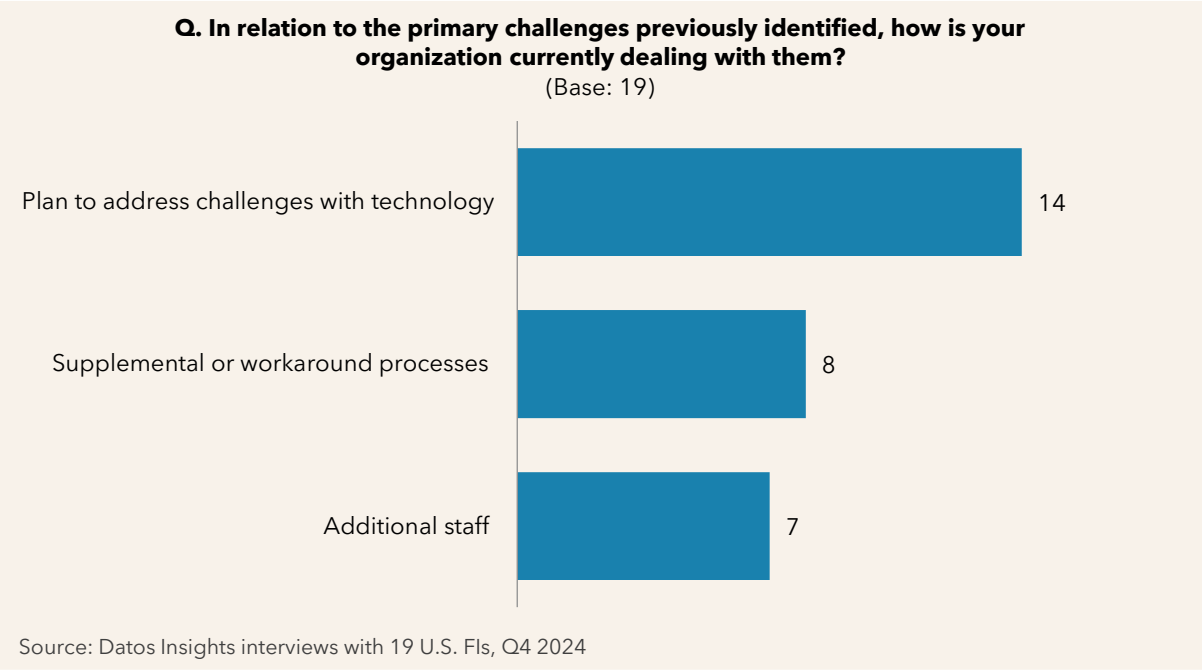
Further, fraud prevention leaders report that their teams often identify new fraud patterns but struggle to implement detection and prevention measures quickly enough. Coordinating changes across multiple systems and channels further slows response times, creating windows of vulnerability that fraudsters can exploit.

Responses and Coping Strategies

FIs are taking a multifaceted approach to address their technological shortcomings, with a clear preference for long-term technical solutions over temporary fixes.

Most FIs indicate that they plan to address their challenges with technology investments (Figure 2). Many organizations are also employing interim measures while these technological initiatives are being approved, developed, and implemented. Approximately 42% of institutions put supplemental or workaround processes in place, while others added incremental staff to help manage their technology gaps. Several FIs are taking multiple approaches.

Figure 2: Response to Technology Obstacles



Source: Datos Insights interviews with 19 U.S. FIs, Q4 2024

Technology Investment Planning

Many organizations are planning technology transformations to address fraud prevention needs. However, securing funding for these initiatives often proves challenging, as fraud prevention competes with other strategic priorities for limited resources. FIs often find themselves balancing immediate tactical needs with longer-term strategic investments, creating complex planning problems.

The approach to technology investment varies significantly based on institutional size and complexity. Larger institutions often pursue comprehensive transformation programs, while smaller organizations typically take a more targeted approach.

Tactical Workarounds and Manual Processes

Many institutions have increased their fraud teams to compensate for technology limitations; others have implemented manual review processes and workarounds. These tactical approaches provide short-term relief but often prove unsustainable as transaction volume and fraud complexity increase. Organizations are in a cycle of adding staff and creating new procedures to address gaps their technology cannot handle.

The reliance on tactical solutions often creates additional barriers around consistency and scalability. Manual processes introduce variability in fraud detection and response while

also limiting the ability to handle growing transaction volume effectively. The cost of maintaining expanded fraud teams and managing complex manual processes strains operational budgets, pushing organizations to seek more sustainable solutions.

Resource Allocation Issues

The industry is dealing with the issue of allocating resources effectively for fraud prevention, and some institutions are struggling to find and retain staff with the necessary technology expertise. The shortage of skilled technical staff often impairs an organization's ability to develop, implement, and maintain advanced fraud prevention capabilities in a legacy environment. Organizations often find themselves competing for limited talent while also trying to maintain existing operations with constrained resources. Coupled with the cost of maintaining expanded fraud teams to compensate for technology gaps, this creates significant resource allocation and cost issues.

Orchestration Solution Adoption

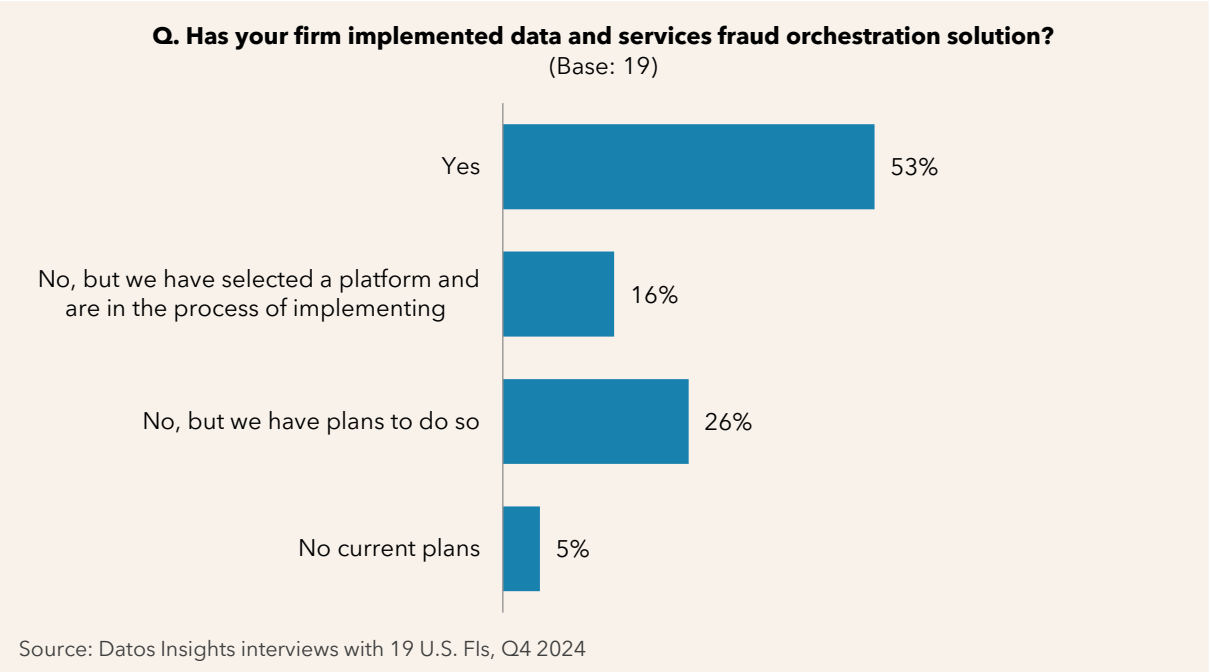
Fraud orchestration solutions present a promising response to a vexing problem. When done correctly, orchestration platforms enable FIs to coordinate multiple fraud point solutions and data sources while delivering real-time detection and interdiction capabilities across multiple channels.

By providing a centralized platform for managing fraud prevention across channels and systems, orchestration solutions help FIs address the fundamental concerns of fragmented detection capabilities. However, implementation often proves complex, requiring significant upfront investment in technology integration.

Adoption and Implementation Patterns

Fraud orchestration adoption varies across the financial services industry. Approximately 53% of institutions have already implemented these solutions, while another 16% have selected a platform and are in the process of implementing them (Figure 3).

Figure 3: Implementation of Fraud Orchestration Solutions



Source: Datos Insights interviews with 19 U.S. FIs, Q4 2024

The remaining organizations are either planning to implement a solution (26%) or have no current plans (5%). This pace of adoption reflects a growing recognition that traditional fragmented approaches to fraud prevention no longer suffice in today's dynamic threat environment.

Most FIs that have implemented fraud orchestration solutions have taken a targeted or phased approach rather than attempting comprehensive coverage from the start. Many have focused initially on specific high-priority areas such as account onboarding or digital authentication and often for select product types. Doing so helps to focus the initial implementations while proving value and gaining experience. This approach also minimizes the opportunity for disruption to existing processes and customers.

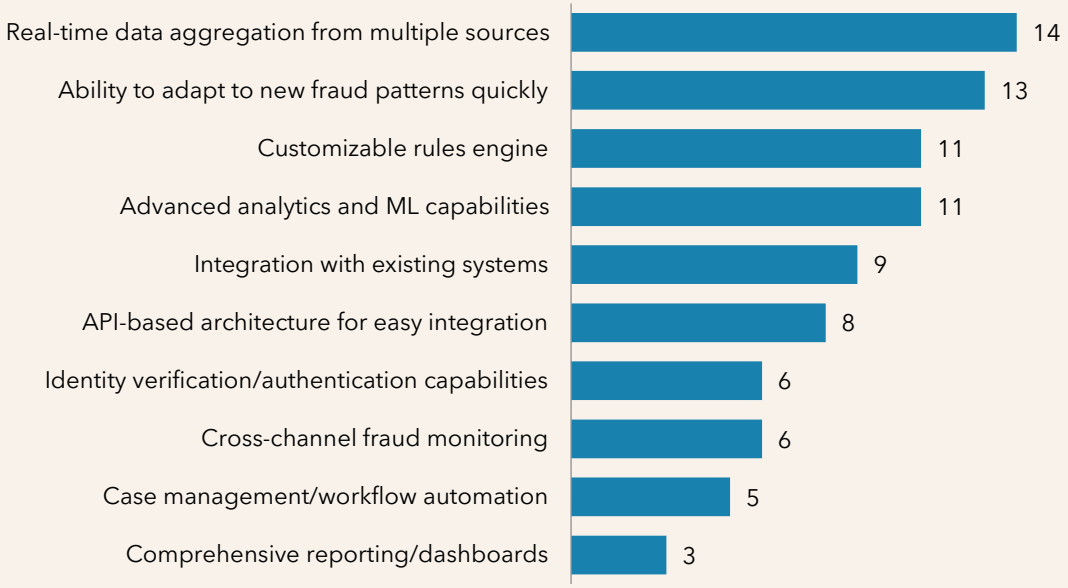
Still, a segmented approach comes with potential issues. Institutions can find themselves with partial orchestration capabilities that don't fully address their broader fraud prevention needs. This reality has led many institutions to plan for expanded implementations that will gradually bring more fraud prevention functions under a unified orchestration framework. However, such expansions often face competition for resources and attention against other strategic priorities.

Key Features and Capabilities

Real-time data aggregation from multiple sources ranks as the most important feature, cited by 74% of respondents, closely followed by the ability to adapt quickly to new fraud patterns (Figure 4).

Figure 4: Fraud Orchestration Solution Features

Q. Which of the following fraud orchestration solution features are most important to your organization?
(Base: 19)



Source: Datos Insights interviews with 19 U.S. FIs, Q4 2024

This emphasis on speed and adaptability reflects the increasingly dynamic nature of fraud threats and the need for FIs to respond rapidly to emerging attack vectors. The strong preference for these capabilities aligns with the growing sophistication of fraudsters who can quickly modify their tactics to exploit new vulnerabilities.

The next priorities focus on sophisticated detection and analysis capabilities, with customizable rules engines and advanced analytics/ML capabilities sharing equal importance. Integration capabilities also emerged as a significant factor, including the integration with existing systems, like core banking and digital banking platforms, and the importance of API-based architecture for easy integration. The emphasis on integration capabilities amplifies the idea that FIs are seeking to avoid creating new silos while implementing new solutions.

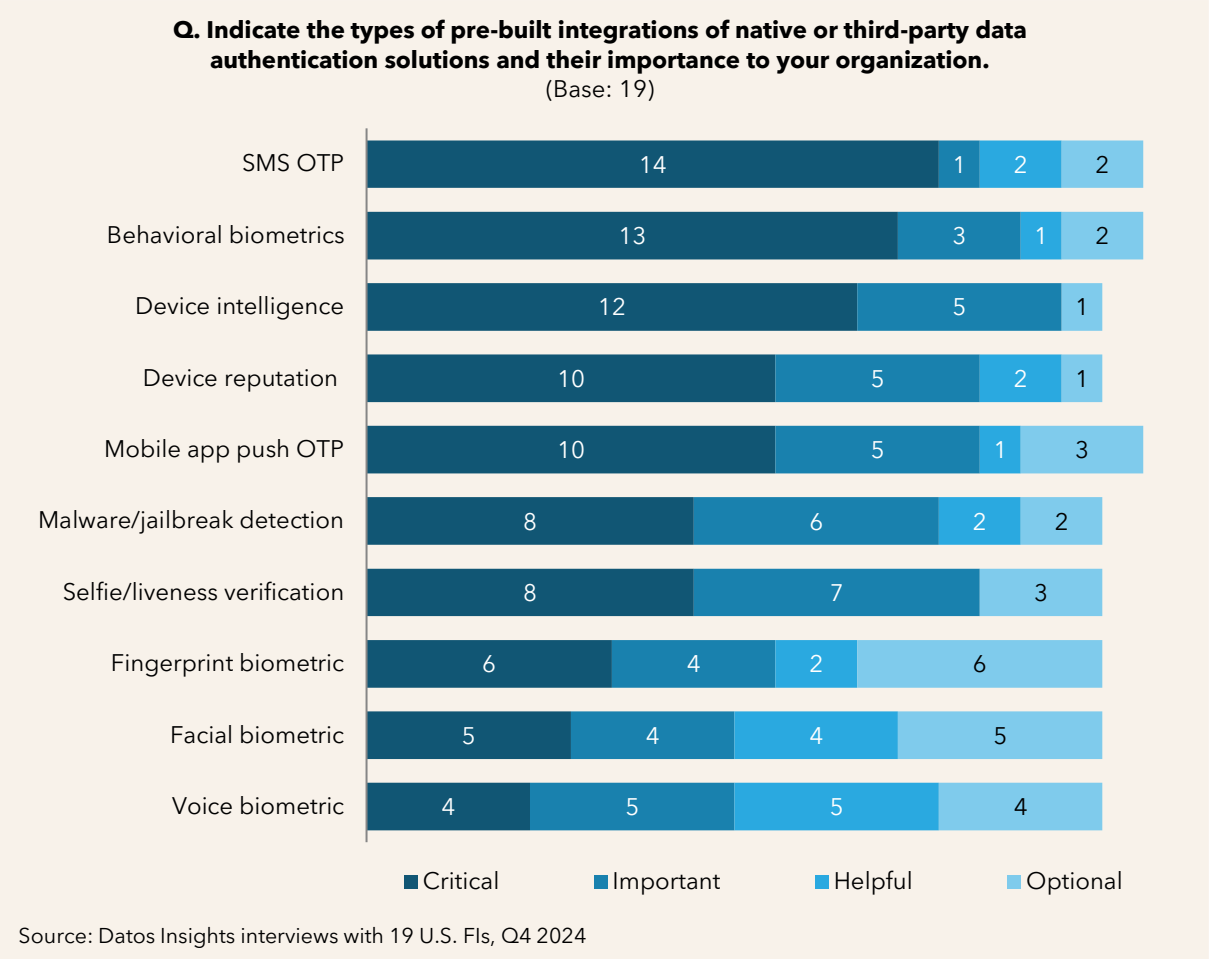
Identity verification/authentication capabilities and cross-channel fraud monitoring are often discussed as critical components of fraud prevention. However, FIs ranked them lower in this study. Case management and comprehensive reporting and dashboards are also ranked as lower priorities, but that appears to reflect the core of what problems FIs are looking to solve with an orchestration tool—the integration of data sources and decisioning to move to real-time risk mitigation.

Moreover, FIs are more focused on core detection and response capabilities rather than operational features, as the relatively low prioritization of reporting and dashboards indicates in many cases that they are planning to leverage existing business intelligence tools rather than rely on native reporting capabilities within fraud orchestration solutions.

Authentication Point Solutions

There is a clear hierarchy in the perceived importance of different authentication solutions for fraud orchestration platforms. FIs are particularly focused on authentication methods that can be deployed at scale while maintaining strong security standards. Traditional SMS one-time passcodes (OTP) remain the most critical authentication method, with 74% of institutions rating it as critical and only 11% considering it optional (Figure 5).

Figure 5: Authentication Solution Integration Importance



Source: Datos Insights interviews with 19 U.S. FIs, Q4 2024

SMS OTP was closely followed by behavioral biometrics, device intelligence, and device reputation. These findings indicate that FIs are generally prioritizing authentication

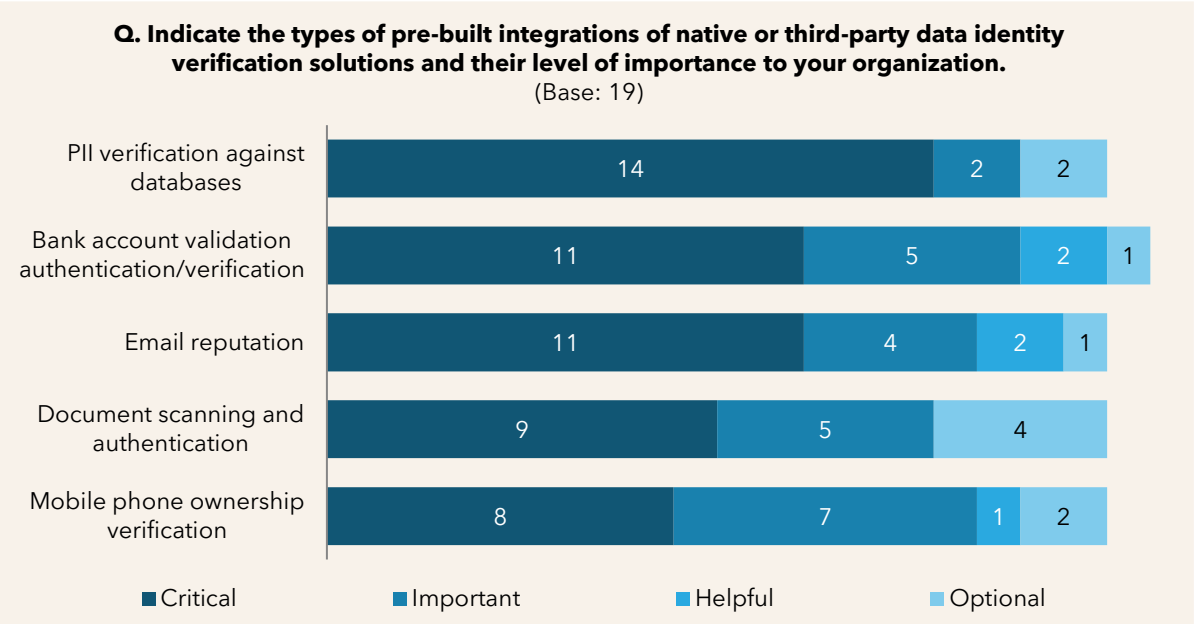
methods that provide strong security while minimizing customer friction. The continued importance of SMS OTP, despite its known vulnerabilities, reflects its universal accessibility and customer familiarity, while the strong interest in behavioral biometrics signals a growing recognition of the need for passive authentication methods that can operate continuously in the background.

The data shows a notable drop-off in perceived criticality for physical biometric solutions. While selfie/liveness verification is still considered critical or important by 79% of institutions, traditional biometric methods such as fingerprint, facial, and voice authentication are viewed as less crucial, with only four to six institutions rating them as critical. These results may reflect the operational hurdles of implementing these solutions and the fact that many institutions leverage device-native biometric capabilities rather than building their own.

Identity Verification Point Solutions

Identity verification solutions show a clear pattern of prioritization, with the verification of personally identifiable information (PII) against other databases emerging as the most critical capability. An overwhelming 14 institutions rated PII verification against databases as critical, with only four institutions considering it merely helpful or optional (Figure 6).

Figure 6: Identity Verification Solution Integration Importance



Source: Datos Insights interviews with 19 U.S. FIs, Q4, 2024

These strong preferences reflect the foundational role that the use of this type of independently sourced data plays in fraud prevention and regulatory compliance, particularly as FIs face increasing pressure to validate customer identities accurately while maintaining efficient onboarding processes.

Bank account validation and email reputation services form the next level of priority, with 57% of institutions rating each as critical. Both solutions show strong overall importance, with 84% of institutions rating bank account validation as either critical or important and 79% of institutions giving the same ratings to email reputation services. This high prioritization echoes the growing importance of digital account opening and payment channels, in which these verification methods serve as key fraud prevention tools.

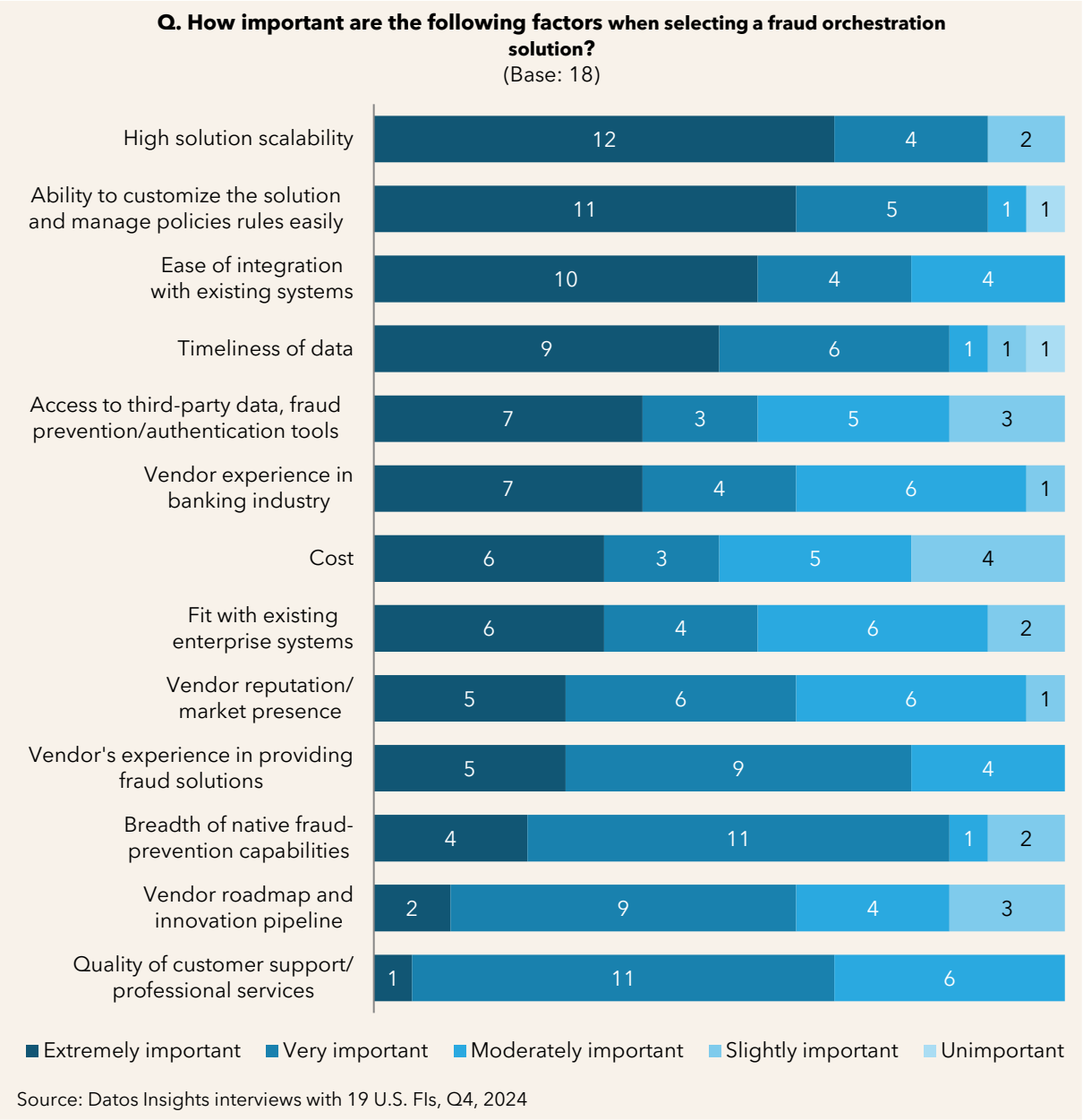
Document scanning/authentication and mobile phone ownership verification, while still important, were rated as critical by fewer institutions (nine and eight, respectively). However, both solutions show strong overall importance when combining critical and important ratings. Fourteen institutions rated document scanning/authentication as either critical or important, and 79% rated the same for mobile phone ownership verification.

These findings suggest that while these capabilities are valuable components of a comprehensive identity verification strategy, FIs may view them as supplementary solutions or step-up tools rather than core requirements. The relatively lower prioritization of document scanning might also reflect the operational complexity and customer friction associated with document-based verification processes, as well as the increasing preference for digital-first verification methods that can deliver results with less customer participation.

Platform Selection Factors

The considerations for selecting fraud orchestration solutions reveal that technical capabilities and operational flexibility are paramount concerns for FIs. High solution scalability and the ability to customize solutions and manage rules easily emerged as the most critical factors, with 67% and 61% of institutions, respectively, rating these as extremely important (Figure 7). This strong emphasis on scalability and customization reflects institutions' need for solutions that can grow with their business while maintaining the flexibility to adapt to evolving fraud threats and business requirements.

Figure 7: Solution Selection Factors



Source: Datos Insights interviews with 19 U.S. FIs, Q4, 2024

Integration and real-time capabilities rank as other top priorities in the selection process. Ease of integration with existing systems was rated as extremely important by 56% of institutions, while timeliness of data was deemed extremely important by half of the institutions. These priorities underscore the critical nature of seamless system integration and real-time data access in advanced fraud prevention strategies. The high prioritization of these factors suggests that institutions are particularly focused on minimizing internal

development resources and ensuring their fraud prevention capabilities can operate at the speed required by today's digital transactions.

Vendor characteristics show a more nuanced pattern of importance. While vendor experience in banking and access to third-party data/tools were rated as extremely important by seven institutions each, factors such as vendor reputation and market presence received more mixed ratings. Interestingly, the vendor's roadmap and innovation pipeline were rated as extremely important by only two institutions, though nine rated it as very important. This result indicates that while institutions value proven expertise and current capabilities, they may be more focused on immediate operational needs than future innovation potential.

The quality of customer support and professional services, along with the breadth of native fraud prevention capabilities, were more likely to be rated as very important rather than extremely important. However, these factors still show strong overall importance, with virtually no institutions rating them as slightly or not at all important. Cost considerations show a surprisingly distributed pattern of importance, with six institutions rating it as extremely important but nearly as many rating it as only moderately or slightly important.

With few exceptions, FIs revealed that they are more interested in the overall return from an orchestration solution based upon realized benefits such as lower fraud rates, operational cost reductions, and customer satisfaction vs. the pure cost of the platform.

Orchestration Benefits

FIs that have implemented fraud orchestration solutions report significant benefits across multiple operational dimensions. Three clear leading benefits emerge, with seven out of 10 respondents citing reduced fraud losses, increased operational efficiency, and improved fraud-detection rates as the most common benefits (Figure 8). While reduced losses and better detection rates generally go hand-in-hand, the duality of achieving a lower level of fraud while enjoying operational savings is powerful.

Figure 8: Realized Benefits of Fraud Orchestration Solutions

The next area of benefits focuses on the accuracy and speed of fraud-detection processes. Five institutions reported reduced false positives, while four cited enhanced real-time decision-making capabilities. These improvements in accuracy and speed are particularly noteworthy as they directly influence operational costs and customer experience. Reduced false positives mean fewer legitimate customers are inconvenienced by unnecessary fraud alerts or transaction delays while reducing the operational burden on staff that must review and clear these alerts.

Customer experience benefits arise as another important outcome of orchestration solution implementation. This suggests that better differentiating between legitimate and fraudulent activity improves customer satisfaction even if customer experience may not be a primary implementation driver. Moreover, better real-time decision-making capabilities likely enhance customer experience by reducing friction for legitimate transactions.

Interestingly, only one institution cited traditionally emphasized benefits of fraud orchestration solutions—improved cross-channel visibility and regulatory compliance. This could indicate that these benefits may be harder to measure, may take longer to realize, or institutions are still in the early stages of leveraging orchestration solutions across channels. Several institutions shared that their implementation approaches focused on specific channels or processes initially before rolling out more broadly. This approach is wise, but it would have an impact on cross-channel visibility until fully implemented.

Looking Forward: Emerging Threats and Trends

The fraud landscape is undergoing a dramatic transformation, driven by the rapid acceleration of digital banking and the emergence of more sophisticated technological threats. As FIs expand their digital offerings and real-time payment capabilities, fraudsters exploit these new channels with increasingly advanced attack methods.

The rise of generative AI technology has created renewed concerns regarding social engineering and impersonation attacks, while the speed of digital transactions has reduced the window for fraud detection and prevention. This technological arms race is particularly evident in the surge of scams targeting digital banking customers, wherein fraudsters combine social engineering with technology to create highly convincing scenarios that bypass traditional fraud controls.

Banks are responding to these evolving threats with increased investment in advanced fraud prevention technologies, particularly AI/ML solutions. However, the issue extends beyond mere technological capabilities. Successful fraud prevention requires a holistic approach that combines improved analytics and broader data accessibility. The rise of fraud orchestration platforms reflects this need for a more comprehensive and coordinated approach to fraud prevention—one that can adapt quickly to new threats while maintaining seamless customer experiences across all channels.

AI and Emerging Technologies

The impact of AI and related technologies creates both opportunities and roadblocks to fraud prevention. FIs express overwhelming concern about the impact of AI and generative AI on social engineering payment scams, with 89% of surveyed institutions identifying this as a key threat vector (Figure 9). This near-unanimous concern reflects the growing sophistication of scams that leverage AI technologies to create more convincing and personalized social engineering attacks. The ability of generative AI to craft highly persuasive communications and potentially clone voices or create deepfake videos makes these types of scams increasingly more difficult for both customers and FIs to detect and prevent.

Figure 9: Impact of AI and Generative AI on Fraud Vectors

Source: Datos Insights interviews with 19 U.S. FIs, Q4 2024

Synthetic identity fraud and business email compromise (BEC) emerge as the second and third most important areas of AI-enhanced threats, with 63% of institutions identifying each as a significant concern. The high ranking of synthetic identity fraud likely reflects concerns about generative AI's ability to create and curate more convincing fictional identities by combining elements from multiple real identities and generating consistent false documentation. Similarly, the focus on BEC attacks is due to institutional worries about AI's potential to make these attacks more sophisticated through improved impersonation capabilities and more convincing communication patterns.

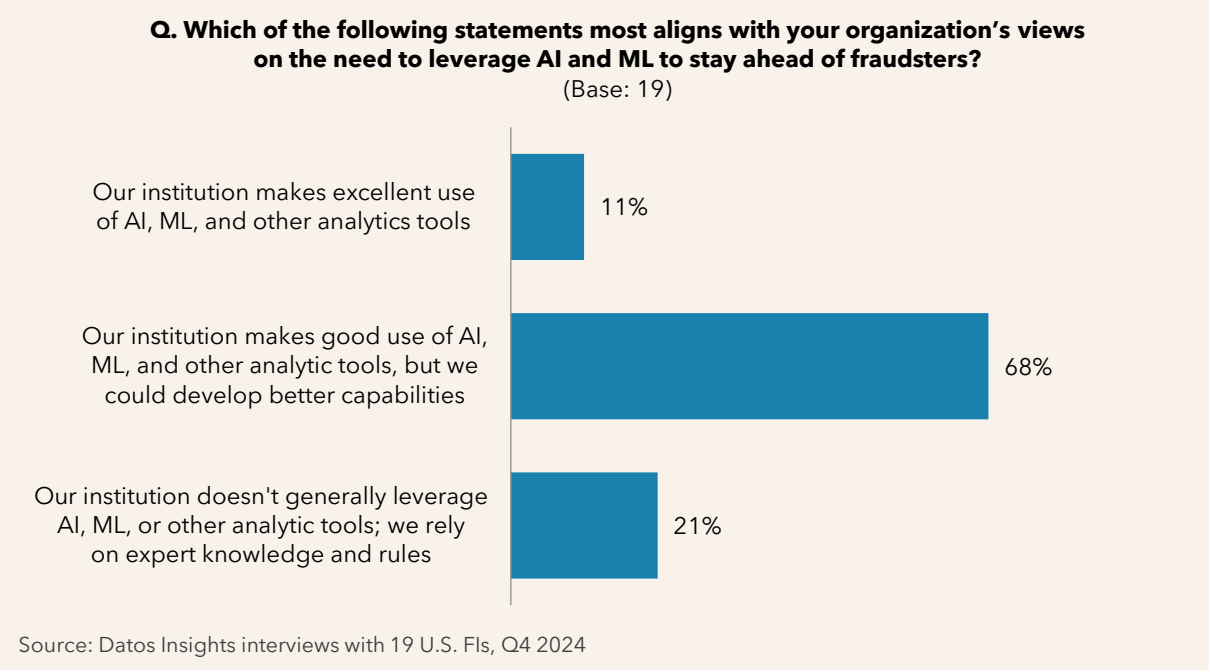
Identity theft through application fraud attacks ranks as the fourth area of concern, with nine institutions identifying this fraud type as vulnerable to AI enhancement. This is followed by session hijacking and remote-access Trojan attacks, cited by seven institutions, and conventional account takeover attacks, mentioned by six institutions. This ranking suggests that, while these traditional attack vectors remain concerning, institutions believe that either the impact of AI will be minimal or that they have better controls in place to detect and prevent these types of fraud, even when enhanced by AI.

Notably, email interception/infiltration and aggregator attacks were cited by only three institutions as being vulnerable to AI enhancement. This lower level of concern might be due to institutional views that these attack vectors as either well-defended or less likely to benefit significantly from AI capabilities. However, the overall pattern of responses suggests that FIs are most concerned about AI's potential to enhance social engineering and identity-based fraud, particularly in attacks that target customers directly rather than attempting to compromise institutional systems.

Making Use of AI in Fraud Prevention

Organizations increasingly recognize the need to adapt their fraud prevention strategies to address AI-powered threats and to use AI as a tool. A significant majority (68%) of FIs surveyed indicate they are making "good use" of AI, ML, and other analytical tools while acknowledging room for improvement in their capabilities (Figure 10). These findings suggest that most institutions have moved beyond basic implementation and are actively employing AI solutions, but they recognize they haven't yet maximized the technology's potential for fraud prevention.

Figure 10: Usage of AI and ML in Fraud Prevention



Source: Datos Insights interviews with 19 U.S. FIs, Q4 2024

Only 11% of respondents believe they are making excellent use of AI/ML tools, highlighting how few institutions feel they have truly mastered these technologies. This relatively low percentage of institutions claiming excellence may reflect the rapidly

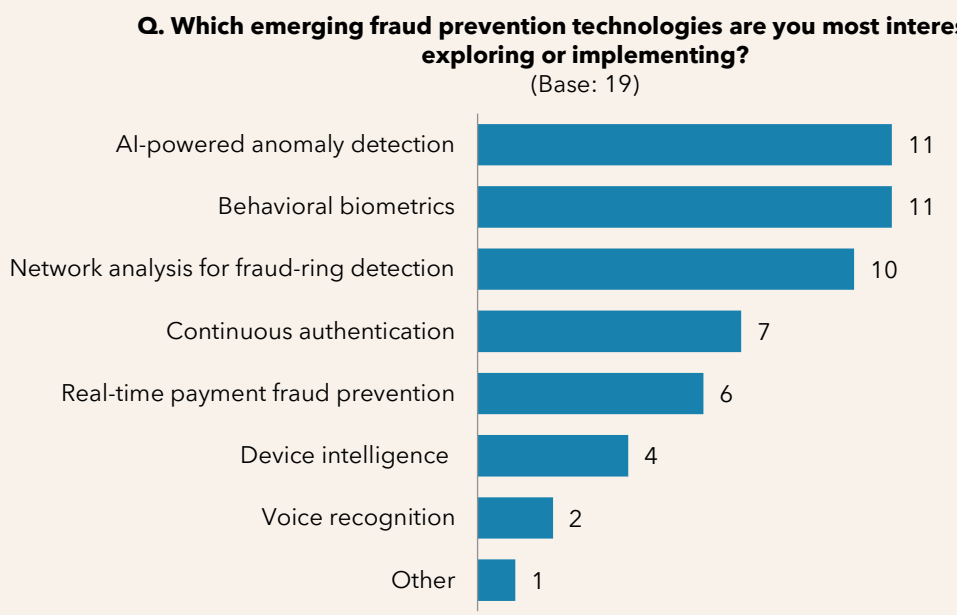
evolving nature of AI technology as well as the growing sophistication of fraud threats that require constant adaptation of defensive capabilities.

At the other end of the spectrum, 21% of institutions report they do not generally leverage AI/ML, instead relying primarily on expert knowledge and rules-based systems. This substantial minority indicates that while AI adoption is widespread, a significant segment of the financial services industry has yet to meaningfully incorporate these technologies into their fraud prevention strategies. The persistence of this gap in AI adoption could create vulnerabilities as fraudsters increasingly leverage advanced technologies in their attacks.

Leading-Edge Fraud Prevention Capabilities

As FIs face an increasingly complex fraud threat landscape, they are strategically evaluating various emerging technologies to enhance their fraud prevention capabilities. The greatest interest is in AI-powered anomaly detection and behavioral biometrics, with both technologies garnering interest from 11 out of 19 surveyed institutions (Figure 11). FIs recognize the potential of both automated, AI-driven analysis and human behavior-based security measures as critical components of their future fraud prevention strategies.

Figure 11: New Technology Implementation



Source: Datos Insights interviews with 19 U.S. FIs, Q4 2024

Network analysis for fraud-ring detection follows closely behind, with 10 institutions expressing interest in exploring or implementing this technology. This strong showing indicates that FIs are increasingly focused on identifying coordinated fraud attempts and understanding the connections between potentially fraudulent activities rather than just examining individual transactions in isolation. The high prioritization of network analysis tools shows a growing recognition that modern fraud schemes often involve sophisticated criminal networks that require equally sophisticated detection methods.

Continuous authentication and real-time payment fraud prevention occupy the middle areas of interest, with seven and six institutions, respectively, expressing interest in these technologies. The moderate level of interest in these areas may reflect the growing importance of seamless security in digital banking and the increasing adoption of real-time payment systems, though implementation problems or competing priorities could be tempering immediate enthusiasm. This measured interest might also indicate that institutions are taking a pragmatic approach to implementation, recognizing that these technologies require significant infrastructure changes and careful integration with existing systems.

At the lower end of the spectrum, device intelligence, voice recognition, and other technologies attracted less interest. This lower prioritization might indicate that these technologies are viewed as more mature solutions that institutions have already implemented or that they are perceived as less critical to addressing current fraud prevention obstacles. The relatively low interest in voice recognition is particularly noteworthy given the rising concerns about voice-based fraud attacks. This pattern suggests that institutions may be concentrating their resources on technologies they view as offering the highest return on investment in the current threat landscape.

Conclusion

The financial services industry stands at a critical juncture in fraud prevention, facing unprecedented struggles from both technological advancement and evolving criminal tactics. FIs that are looking to enhance their fraud prevention capabilities with orchestration capabilities should consider the following:

- **Prioritize the consolidation of fraud-related data sources through orchestration.** Failing to address data fragmentation will increase vulnerabilities to sophisticated fraud attacks.
- **Develop a clear roadmap for implementing real-time fraud prevention capabilities across all channels and payment types.** The acceleration of payment speeds and growing customer expectations for immediate transactions make this a critical priority.
- **Employ a phased approach to implementing fraud orchestration.** Starting with high-priority areas while maintaining a vision for comprehensive coverage allows institutions to prove value and gain experience while minimizing disruption.
- **Prioritize the development of ML capabilities and AI.** Focus initially on areas where these technologies can provide immediate value, such as anomaly detection and behavioral analysis. The growing sophistication of fraud attacks, particularly those enhanced by AI, makes these capabilities crucial.
- **Invest in automated workflow solutions to reduce reliance on manual processes and free up fraud prevention staff for higher-value activities.** The combination of growing transaction volume and increasing fraud complexity makes manual approaches increasingly unsustainable.
- **Establish clear metrics for measuring the effectiveness of fraud prevention investments.** Include direct impacts on fraud losses and broader operational benefits, such as reduced operations cost. This approach will help justify continued investment in fraud prevention capabilities while ensuring resources are allocated effectively.

The path forward in fraud prevention requires a delicate balance between technological advancement and operational pragmatism. While the issues are significant, institutions that take a strategic approach to modernizing their fraud prevention capabilities while maintaining operational effectiveness will be best positioned in an increasingly complex and challenging environment.

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