Fall 2025

Liminal

Friendly ACH in Banking

First Party Fraud

link Index™ Report

Contents

Navigation – click the Liminal logo to return to this page.

Introduction

MarketOverview 3

Vendor Landscape 5

Use Case Overview 7

Market Overview: Friendly ACH in Banking 8

Liminal's Use Case Methodology: Key Product Requirements 9

Friendly ACH Buyer Personas 11

Chief Information Security Officer (CISO) 12

Chief Risk Officer (CRO) 13

Head of Payments 14

End-to-End Solutions Prevent ACH Fraud, Detect Risky Transactions, and Safeguard Merchants From Costly Disputes 15

Market Overview 16

Friendly ACH Key Insights 17

Friendly ACH Operational Barriers 18

Key Purchasing Criteria for Friendly ACH Solutions 19

Friendly ACH in Banking: Market Evolution 20

Link Index 21

Friendly ACH Vendor Product Evaluation 22

Friendly ACH Vendor Strategy Evaluation 24

Friendly ACH Vendor Market Presence Evaluation 25

Friendly ACH in Banking: Vendor Evaluation 26

Friendly ACH: Leading Vendors 29

15 Leaders, 34 Evaluated Vendors 30

Link Index Leading Vendors for Friendly ACH Fraud in Banking in 2025 31

Friendly ACH Leading Vendor Characteristics 32

Friendly ACH Leading Vendor Future Outlook 33

Vendor Overviews 34

Unit21 35

Appendix 38

Market Presence Survey Demographics 39

Link Index Methodology: Exceptional, Excellent, Strong Scoring Buckets Definitions 40

Product Capability Definitions 41

Link Index Methodology: Product 45

Link Index Methodology: Strategy 46

Link Index Methodology: Market Presence 47

About Liminal 48

Market Overview

Key Takeaways

74%

of institutions favor hybrid approaches that combine rules-based and AI/ML detection

79%

of practitioners expect real-time return code analysis in fraud systems

100%

of professionals report mismatches when working with peers

01

Codified Taxonomies Reduce Friction in ACH Fraud Classification[1]

First-party fraud lacks consistent classification. While 95% of practitioners use codified taxonomies, the mix of proprietary and industry-specific standards causes fragmentation. As a result, 100% of professionals report mismatches when working with peers, complicating benchmarking, reporting, and collaboration.

02

Hybrid Fraud Detection Models Gain Momentum[1]

Rules-based systems are rigid, with 66% citing poor adaptability and 48% facing high false positives. AI/ML tools offer advantages such as contextual insights (69%), reduced rule maintenance (65%), and faster pattern recognition (57%). This has driven 74% of institutions to favor hybrid approaches that combine rules-based and AI/ML detection, making adaptability the primary driver of demand.

03

Real-Time Return Code Data Integration Becomes Essential[1]

With NACHA expanding return code usage, 79% of practitioners expect real-time return code analysis in fraud systems. Dashboards and reporting are also sought for visibility into ACH return trends. Buyers increasingly want automated processing with actionable insights, positioning return code integration as a core requirement.

1 First Party Fraud Buyer Demand Survey, July 2025 (N=58)

Market Overview

Current Challenges[1]

Delayed Detection and Manual Review Create Strain

Although 72% of practitioners can act within minutes, 47% still report detection delays that limit real-time response. Manual review adds pressure, with 60% identifying it as a constraint on operations, underscoring the need for faster, automated tools.

Limited AI/ML Transparency Slows Adoption

AI/ML systems improve adaptability and decisioning but often lack explainability. Only 16% of practitioners see transparency as a benefit, compared to 51% for scalability and 69% for contextual insights. Without interpretability, compliance and trust concerns slow adoption.

Reliance on Basic Features Restricts Advancement

Most practitioners rely on IP address logging (84%) and device fingerprinting (83%). Advanced techniques remain limited, with only 31% using keystroke dynamics and 34% adopting FIDO2 passkeys. Dependence on baseline tools restricts authentication innovation.

Future Demands[1]

Real-Time Processing to Define Next-Gen Detection

Sixty-two percent of practitioners see real-time detection as the most impactful advancement within two years. Faster processing will allow intervention before funds move, reducing exposure to first-party fraud. Vendors that deliver real-time capabilities are positioned to lead adoption.

Codified Taxonomies to Expand Standardization

Access to detailed data from payment providers will rise. Currently, 28% of practitioners receive comprehensive NACHA reason codes with metadata; this is projected to reach 41% in two years. Expanded access will reduce mismatches and foster consistent analysis across institutions.

Budget Growth and Vendor Expansion Expected

Budgets for ACH fraud prevention are projected to grow 10% annually, while vendor use is expected to expand by 25%. Organizations are diversifying providers for broader coverage, though rising costs may drive consolidation over time.

Leading Key Purchasing Criteria (KPC) for Friendly ACH Solutions[1]

Scalability

98% of friendly ACH practitioners consider scalability important when selecting a solution.

Data Quality

98% of friendly ACH practitioners consider data quality important when selecting a solution.

Accuracy

97% of friendly ACH practitioners consider accuracy important when selecting a solution.

1 First Party Fraud Buyer Demand Survey, July 2025 (N=58)

Vendor Landscape

Liminal's Friendly ACH Fraud in Banking vendor landscape analysis identifies the top 15 vendors addressing the complexity of verifying real-world identities in digital environments.

Practitioners face operational strain from delayed detection and manual reviews, limited adoption of opaque AI/ML systems, and overreliance on basic authentication tools—highlighting the urgent need for faster, more transparent, and advanced fraud detection technologies. Vendors within this landscape offer specialized approaches, categorized into four primary groups: End-to-End Fraud and AML Platforms, Fraud Detection and Risk Analytics Platforms, Authentication and Identity Intelligence Providers, and Specialized ACH Dispute and Workflow Solutions.

Landscape Analysis

End-to-End Fraud and AML Platforms

These vendors offer comprehensive solutions for ACH fraud prevention, integrating real-time transaction monitoring, behavioral analytics, risk scoring, and AML compliance tools within broader anti-fraud frameworks. Serving banks and large financial institutions, their platforms unify fraud detection, KYC, and transaction risk management for unified oversight and regulatory alignment.

Fraud Detection and Risk Analytics Platforms

Platforms specializing in identifying first-party and friendly ACH fraud use adaptive analytics, hybrid detection models, and data enrichment. They leverage machine learning, behavioral biometrics, and real-time return code analysis to detect fraudulent dispute patterns. Scalable and integrable, these platforms are for mid-sized institutions needing strong detection without full AML infrastructure.

Authentication and Identity Intelligence Providers

Vendors in the ACH ecosystem enhance authentication and user verification through biometrics, MFA, and device/behavioral profiling to confirm legitimate account holders and reduce unauthorized access. Many integrate with fraud monitoring to prevent friendly fraud during transactions or dispute filings.

Specialized ACH Dispute and Workflow Solutions

These vendors automate dispute management for ACH returns and reversals, offering audit trails and streamlining investigations. Their systems unify transaction and customer data, ensuring NACHA compliance. Ideal for institutions with high dispute volumes, these solutions enhance efficiency, data quality, and traceability, reducing manual review burdens.

Vendor Landscape

Leading Vendors for Friendly ACH Fraud in Banking

ACI Worldwide
AppGate
DATAVISOR
EQUIFAX
feedzai
FICO
FraudNet
Nasdaq Verafin
NICE Actimize
OUTSEER
Sardine
SEON
sift
Unit21
VISA

01

Use Case Overview

Market Overview: Friendly ACH in Banking

Friendly ACH fraud impacts banks as account holders dispute authorized payments after receiving benefits. AI-based detection and real-time analysis help reduce losses and protect trust

Friendly ACH fraud in banking occurs when an account holder initiates a payment and later disputes the charge, falsely claiming it was unauthorized despite receiving the benefit of the transaction. This form of first party fraud exploits the trust inherent in ACH transactions, where the account holder is assumed to act in good faith. Because the fraud is committed by the legitimate account holder, it is more difficult to detect and prove than traditional unauthorized fraud.

Addressing friendly ACH fraud is essential for financial institutions to prevent revenue loss and operational inefficiencies caused by fraudulent disputes of authorized transactions. Banks must strengthen detection systems that can identify patterns such as unusual dispute activity or inconsistencies in transaction histories. Clear communication and education for customers about the implications of disputing legitimate charges can also reduce misuse of dispute processes.

The problem has expanded as digital banking and online payments have increased the convenience of ACH transactions. Many banks still rely on basic controls and manual review, which are not effective against complex fraud patterns. As ACH use grows, institutions face larger volumes of disputes and greater financial risk.

Fraud prevention demand is rising as banks seek to protect the integrity of ACH systems. Increased adoption of digital banking has expanded the attack surface for friendly ACH fraud, while economic pressures have contributed to a higher incidence of fraudulent disputes. Existing fraud detection tools often lack the ability to distinguish genuine disputes from fraudulent claims, creating financial and operational strain.

Technology advances are enabling better detection. AI driven solutions can analyze transaction data in real time to identify anomalies and potential abuse. Integration of advanced fraud tools into banking platforms has made it easier for institutions to deploy effective safeguards. Vendors are also developing scalable options for smaller banks and credit unions, improving access to modern solutions without large upfront investment.

Preventing friendly ACH fraud requires a combination of stronger authentication, pattern recognition, and customer education. Financial institutions that adopt these measures can reduce losses, maintain the trustworthiness of ACH payments, and ensure a fair process for legitimate disputes. Proactive prevention is increasingly critical as digital payment volumes continue to grow.

Liminal's Use Case Methodology: Key Product Requirements

To effectively support Friendly ACH processes, vendors must fulfill eight key product requirements, each encompassing a range of capabilities with varying levels of demand

Eight key requirements outline the product capabilities and technical features needed to solve Friendly ACH. According to our survey, the most sought-after capabilities for solving Friendly ACH are listed below. For a comprehensive mapping of these capabilities to corresponding technical features, please refer to **Link™**. The following scale was used to prioritize capabilities:

- **High:** Capabilities essential for solving the use case
- **Medium:** Helpful capabilities
- **Low:** Capabilities that practitioners do not prioritize

Requirements to Satisfy the Use Case		Buyer Demand for Product Capability[1]
Authenticate Customer Accounts	Verifies that a user accessing a system is the legitimate owner of the account. This typically involves validating identity credentials, such as passwords, multi-factor authentication (MFA), biometric data, or one-time passcodes, at login or during sensitive transactions. The goal is to ensure only authorized users can access or modify account information, protecting against unauthorized access, fraud, and identity theft.	Biometric Authentication ●
		Multi-factor Authentication ●
		App-based Authentication ◉
		Passwordless Authentication ◉
		Continuous Authentication ○
		Mobile Carrier API Access ○
Detect Anomalous Behavioral Activity for Fraud Threats	Analyzes user behavior to identify actions that deviate from typical patterns and may indicate fraudulent intent. By detecting these anomalies in real time, organizations can flag potential first-party, third-party, or synthetic identity fraud before it results in financial loss.	Customer Risk Profiling ●
		Unified Customer View Creation ●
		Behavioral Analytics ◉
		Behavioral Biometrics ◉
		Cross-device Identity Graphing ◉
		Location Intelligence ○
		Mobile Carrier API Access ○
Establish a Customer Identity Profile for Fraud Detection	Aggregates and unifies identity-related data from multiple sources into a single, comprehensive profile for each customer. This includes personal identifiers, account relationships, device usage, behavioral patterns, and historical transactions. The unified profile supports real-time decision-making, improves risk scoring, and reduces false positives in fraud detection systems.	Customer Data Collection & Integration ●
		Data Enrichment ●
		Unified Customer View Creation ●
		Cross-device Identity Graphing ◉
		Identity Resolution ◉
		Cross-Channel Customer Tracking ○
		Fraud Consortium Data Sharing ○
Detect Suspicious Transactions for Fraud	Analyzes transaction data for anomalies, patterns, and behaviors indicative of fraud. This capability involves monitoring transactions in real-time or near-real-time using rule-based engines, machine learning models, or behavioral analytics to flag unusual activity such as sudden changes in spending, high-risk geographies, or rapid movement of funds.	Dispute Pattern Analysis ●
		Fraud Monitoring ●
		Transaction Fraud Risk Scoring ●
		Behavioral Analytics ◉
		Behavioral Biometrics ◉
		ACH Destination Reputation Scoring ○
		Fraud Consortium Data Sharing ○
		Location Intelligence ○

● High ◉ Medium ○ Low

1 First Party Fraud Buyer Demand Survey, July 2025 (N=58)

Liminal's Use Case Methodology: Key Product Requirements

To effectively support Friendly ACH processes, vendors must fulfill eight key product requirements, each encompassing a range of capabilities with varying levels of demand

Eight key requirements outline the product capabilities and technical features needed to solve Friendly ACH. According to our survey, the most sought-after capabilities for solving Friendly ACH are listed below. For a comprehensive mapping of these capabilities to corresponding technical features, please refer to **Link™**. The following scale was used to prioritize capabilities:

- **High:** Capabilities essential for solving the use case
- **Medium:** Helpful capabilities
- **Low:** Capabilities that practitioners do not prioritize

Requirements to Satisfy the Use Case		Buyer Demand for Product Capability[1]	
Enrich AML Risk Assessments with Transaction Data	Integrates supplementary information, such as geographic location, historical patterns, customer behavior, or third-party intelligence. This enriched data provides deeper insights, enabling more accurate risk assessments and more informed decision-making during transaction monitoring and analysis.	Consumer Financial Transaction Data	◉
Generate a Dynamic User Fraud Risk Score	Calculates a user's likelihood of engaging in fraudulent activity based on both real-time signals and historical behavior. The dynamic nature of the score allows it to evolve with each user interaction, enabling adaptive fraud prevention strategies. This capability helps organizations detect emerging threats, prioritize high-risk users, and apply appropriate controls or interventions.	Customer Risk Profiling	●
		Fraud Monitoring	●
		Transaction Fraud Risk Scoring	●
		Consumer Financial Transaction Data	◉
		Data Enrichment	◉
		Behavioral Analytics	○
		Behavioral Biometrics	○
		Location Intelligence	○
Manage Investigations and Case Workflows	Coordinates the end-to-end process of investigating suspicious activities or incidents. This capability ensures that cases are systematically tracked, documented, and resolved, with clear workflows for assigning tasks, updating statuses, and maintaining records for compliance and audit purposes.	Fraud Alert and Case Management	◉
Document an Audit Trail	Records all actions and changes within a system, providing a detailed log that can be reviewed for compliance, security, and operational transparency. This requirement is essential for tracing the history of transactions, user activities, and system modifications, ensuring accountability and facilitating audits.	Fraud Audit Trail Management	◉

● High ◉ Medium ○ Low

1 First Party Fraud Buyer Demand Survey, July 2025 (N=58)

Friendly ACH Buyer Personas

Friendly ACH fraud prevention involves stakeholders across security, risk, and payments who oversee transaction integrity, fraud controls, and compliance processes

01

Chief Information Security Officer (CISO)

A Chief Information Security Officer (CISO) is responsible for developing and implementing an organization's information security strategy. Their primary responsibilities include safeguarding company data, ensuring compliance with security regulations, managing cybersecurity risks, and leading incident response efforts. As part of the C-Suite, the CISO plays a critical role in aligning security initiatives with business objectives, reporting to the CEO, board of directors, or another high-ranking executive.

02

Chief Risk Officer (CRO)

The Chief Risk Officer is responsible for overseeing and managing the organization's overall risk management strategy. They identify, assess, and mitigate potential risks across all areas of the business, including financial, operational, regulatory, and strategic risks. The CRO ensures that the organization has robust risk management frameworks in place, working closely with other executive leaders to develop policies that minimize risk exposure while supporting the company's long-term goals. They also ensure compliance with relevant laws and regulations, safeguarding the organization's assets and reputation.

03

Head of Payments

The Head of Payments is responsible for overseeing all aspects of payment processing within an organization, including transaction management, system operations, and payment security.
They ensure that payment systems are efficient, reliable, and secure, while also managing relationships with payment service providers and vendors. This role involves developing strategies to optimize payment processes, address any operational issues, and implement solutions that enhance the security and accuracy of transactions across various payment channels.

01 02 03

Chief Information Security Officer (CISO)

A CISO addressing ACH fraud leads security strategy by implementing advanced safeguards, real-time monitoring, and cross-departmental controls to protect transactions and mitigate risk

The Chief Information Security Officer (CISO) oversees the development and implementation of cybersecurity strategies to protect transactions. They ensure that measures, such as encryption, multi-factor authentication, and real-time monitoring, are in place to safeguard against fraudulent activities. The CISO is responsible for coordinating with departments to integrate solutions into the organization's security framework, ensuring compliance with regulatory requirements.

Goals

- Implement Incident Response Plans
- Safeguard Sensitive Organizational Data
- Deploy Security Safeguards
- Mitigate Fraud Risk
- Strengthen Internal Policies and Controls

Needs

- Advanced Threat Detection Tools
- Comprehensive Risk Assessment Tools
- Data Security and Privacy Protections
- Enforcement of Security Policies

Frustrations

- Evolving Threat Landscape
- Budget Constraints
- Delayed Incidence Response
- Disparate Security Tools and Systems
- Cross-departmental Misalignment

Decision Drivers

- Advanced Threat Detection Capabilities
- Integration with Existing Infrastructure
- Proactive Threat Intelligence
- Real-time Monitoring, Alerts, and Reporting
- Detection and Prevention of Fraud

KPCs

- Accuracy
- Automation Capabilities
- Pricing
- Technology Integration
- Data Security

01 02 03

Chief Risk Officer (CRO)

A CRO addressing ACH fraud develops risk frameworks and compliance measures to identify, assess, and mitigate fraud risks while aligning prevention efforts with the organization’s overall risk strategy

The Chief Risk Officer (CRO) oversees the organization’s risk management strategies and ensuring that fraud risks are identified and mitigated. They are responsible for developing and implementing risk assessment frameworks that include fraud prevention measures specific to ACH transactions. The CRO also ensures that the organization adheres to best practices and regulatory requirements related to fraud risk. By collaborating with other departments, the CRO helps integrate fraud prevention efforts into the broader risk management strategy, balancing fraud prevention with overall risk exposure.

Goals

- Mitigate Fraud Risk
- Ensure Regulatory Compliance
- Minimize Financial Crimes Risk
- Enhance Customer Risk Profiling
- Implement Incident Response Plans

Needs

- Unified Customer View
- Integrated Data Analytics
- Integrated Third-party Data Sources
- Regular Compliance Reports
- Comprehensive Risk Assessment Tools

Frustrations

- Inconsistent Data Quality
- Evolving Threat Landscape
- Regulatory Uncertainty
- Cross-departmental Misalignment
- Legacy Technology

Decision Drivers

- Comprehensive Risk Assessment Capabilities
- Detection and Prevention of Fraud
- Return on Investment (ROI)
- Reliable Data Across Systems
- Compliance with Regulatory Requirements

KPCs

- Pricing
- Impact on KPIs & Metrics
- Compliance and Regulatory Alignment
- Accuracy
- Enhanced Reporting

01 02 03

Head of Payments

A Head of Payments addressing ACH fraud deploys monitoring and authentication measures to protect transactions, optimize payment processes, and ensure regulatory compliance

The Head of Payments implements tailored fraud prevention strategies, such as transaction monitoring and enhanced authentication protocols, to safeguard against fraudulent activities. Additionally, they collaborate with security teams to address system vulnerabilities and continuously optimize payment processes. Their role also involves ensuring compliance with industry regulations and best practices for ACH transactions.

Goals

- Mitigate Fraud Risk
- Minimize Financial Crimes Risk
- Drive Operational Efficiency and Effectiveness
- Implement Incident Response Plans
- Ensure Regulatory Compliance

Needs

- Comprehensive Risk Assessment Tools
- Enforcement of Security Policies
- Scalable Technical Infrastructure
- Real-time Alerts
- Integrated Data Analytics

Frustrations

- Evolving Threat Landscape
- Insufficient Threat Monitoring
- Overwhelming Alert Volume
- Disparate Security Tools and Systems
- Complex Systems Integration

Decision Drivers

- Detection and Prevention of Fraud
- Integration with Existing Infrastructure
- Return on Investment (ROI)
- Scalability with Transaction Volume

KPCs

- Accuracy
- Compliance and Regulatory Alignment
- Technology Integration
- Policy Integration and Enforcement
- Real-time Processing

End-to-End Solutions Prevent ACH Fraud, Detect Risky Transactions, and Safeguard Merchants From Costly Disputes

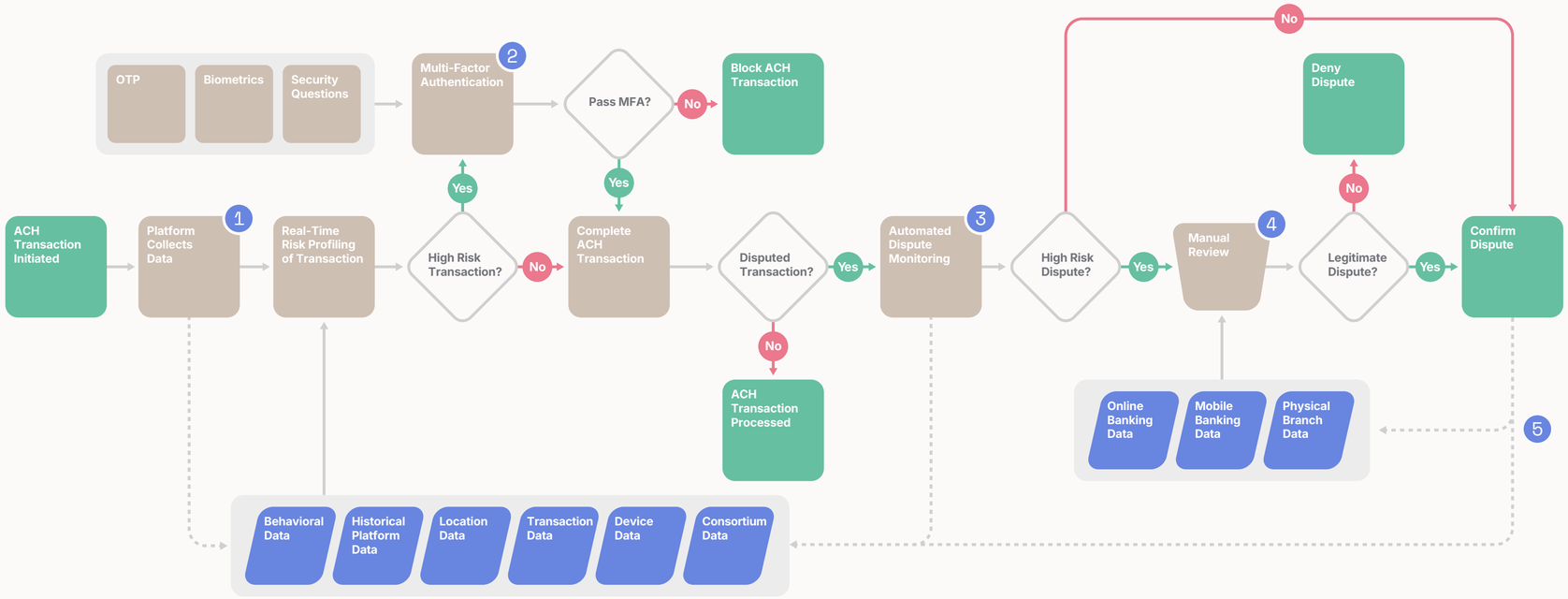
1 Real-Time Monitoring – Analyzing ACH Transactions
As the ACH transaction processes, the system monitors for unusual patterns like large transfers or repeated activity. Machine learning compares the transaction to user behavior and fraud scenarios, updating the risk score as new data is received.

2 Multi-Factor Authentication – Verifying Customer Identity
Before finalizing the ACH transaction, the system may require MFA, such as OTPs, biometrics, or security questions. These extra steps confirm the transaction is authorized by the legitimate account holder.

3 Automated Dispute Detection – Identifying Fraudulent Claims
When a dispute occurs, the system reviews transaction details, risk scores, and alerts. Behavioral analytics and past disputes help determine if the claim is valid, flagging high-risk cases for manual review.

4 Cross-Channel Integration – Creating a Unified Activity View
The system aggregates data from online banking, mobile apps, and branches to detect inconsistencies. By correlating behavior across channels, it identifies patterns that could indicate friendly ACH fraud.

5 Post-Transaction Monitoring – Detecting Ongoing Fraud
After completion, the system monitors for unusual account activity or new disputes. It generates alerts for behavior that deviates from norms, prompting fraud teams to investigate further.



02

Market Overview

Friendly ACH Key Insights

Driving alignment and adaptability in fraud prevention through codified taxonomies, hybrid detection models and real-time data integration

Codified Taxonomies Drive Alignment and Reduce Friction in the Friendly ACH Fraud Landscape

First-party fraud classification lacks consistency. While 95% of professionals use codified taxonomies, the variety of proprietary and industry standards causes fragmentation. This inconsistency leads to 100% of professionals experiencing classification mismatches when collaborating with peers, hindering benchmarking, reporting, and teamwork.[1]

Hybrid Fraud Detection Models Gain Momentum as Institutions Prioritize Adaptability to New Threats

Rules-based systems are rigid and limited. 66% of users report weak adaptability and 48% face high false positives. In contrast, AI/ML models deliver stronger performance, richer contextual insights (69%), reduced rule maintenance (65%), and faster pattern detection (57%). This advantage drives a 74% institutional shift to hybrid models, highlighting adaptability as the key driver.[1]

Real-Time Return Code Data Integration Becomes Essential for Fraud Detection and Transparency

As NACHA expands return code usage, buyers expect vendors to make the data operational. Seventy-nine percent seek real-time return code analysis within fraud detection systems, and want dashboards and reporting for visibility into ACH return trends. Demand is shifting toward solutions that automate processing and provide actionable insights for compliance and risk management teams.[1]

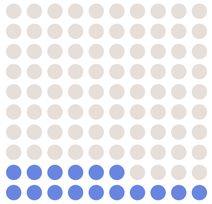
79%

79% of buyers seek real-time return code analysis within fraud detection systems, and want dashboards and reporting for visibility into ACH return trends

1 First Party Fraud Buyer Demand Survey, July 2025 (N=58)

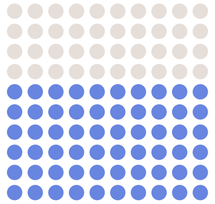
Friendly ACH Operational Barriers

Overcoming operational strain in ACH fraud prevention by addressing delayed detection, manual review, opaque AI systems, and limited technical features



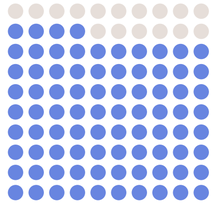
16%

Only 16% of practitioners identified explainability as a benefit of AI/ML systems



60%

of practitioners identify manual review as a key constraint that strains operational capacity and slows response times



84%

of practitioners depend on IP address logging and 83% on device fingerprinting, as baseline tools for ACH transaction risk assessment

Delayed Detection and Manual Review Create Operational Strain in ACH Fraud Prevention Processes

Delayed detection and manual review are significant constraints in ACH fraud prevention. While 72% of practitioners report the ability to act within minutes, this is often insufficient; 47% still cite delayed detection as a primary limitation, suggesting that even a few minutes can be too slow when real-time action is desired. The problem intensifies as 60% identify manual review as a critical bottleneck slowing operations and response.[1]

Heavy Reliance on Basic Technical Features Limits Advancement in ACH Fraud Detection Capabilities

Practitioners heavily depend on baseline tools like IP address logging (84%) and device fingerprinting (83%) for ACH transaction risk assessment. However, the adoption of advanced methods remains low, with only 31% using keystroke dynamics and 34% applying FIDO2 passkeys. This over-reliance on foundational features and limited deployment of advanced techniques restricts progress in fraud detection and user authentication.[1]

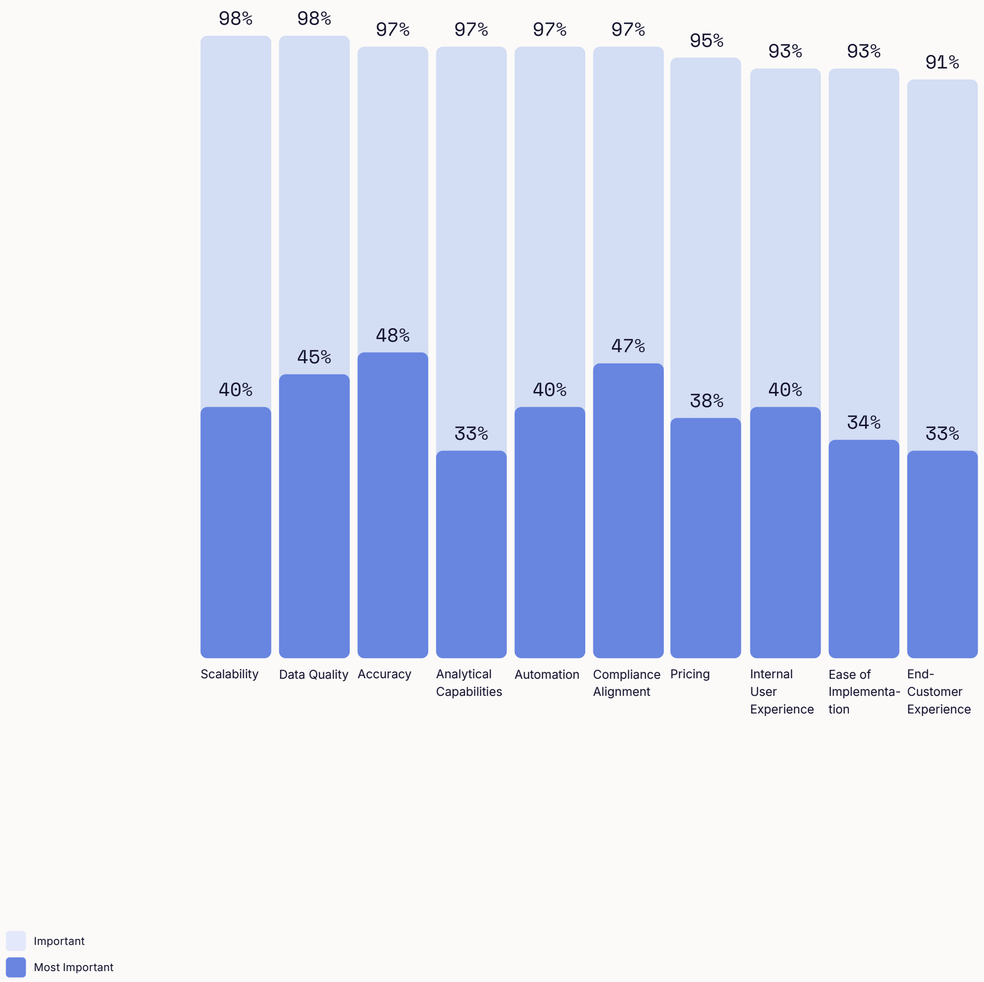
Lack of Transparency and Explainability in AI/ML Fraud Detection Creates Barriers to Adoption

Despite strengthening fraud detection with adaptability and contextual insights, AI/ML systems often lack transparency. Only 16% of practitioners identified explainability as a benefit, significantly less than the 51% for scalability and 69% for contextual decisioning. Without interpretable outcomes, fraud teams face compliance and trust challenges, slowing adoption and raising concerns over reliance on opaque systems.[1]

1 First Party Fraud Buyer Demand Survey, July 2025 (N=58)

Key Purchasing Criteria for Friendly ACH Solutions[1]

Friendly ACH practitioners prioritize scalability, and data quality as the most important criteria in their purchasing process



1 First Party Fraud Buyer Demand Survey, July 2025 (N=58)

Friendly ACH in Banking: Market Evolution

Shaping the future of ACH fraud prevention through real-time processing, standardized taxonomies, expanded budgets and multi-vendor strategies

10%↗

Budgets are projected to grow 10% annually, though this lags vendor adoption

41%↗

of practitioners are projected to receive full NACHA codes with metadata within two years

62%

of practitioners identify real-time detection and alerting as the most impactful advancement for ACH fraud prevention over the next two years

Real-Time Processing Positioned as the Defining Capability for Next-Generation ACH Fraud Detection

Real-time detection and alerting are expected to shape the future of ACH fraud prevention, with 62% of practitioners identifying it as the most impactful advancement over the next two years. Faster processing will allow institutions to intervene before funds are moved, reducing exposure to first-party fraud. Vendors delivering real-time capabilities are likely to lead adoption as demand for immediate response grows.[1]

Codified Taxonomies Expected to Expand Data Access and Standardization in ACH Fraud Management

The importance of standardized taxonomies in ACH fraud classification is expected to rise with greater access to data from payment providers. Currently, only 28% of practitioners receive full NACHA codes with metadata, but this is projected to reach 41% in two years. Expanded data access will improve coding alignment, reduce mismatches, and enable more consistent fraud analysis across institutions.[1]

Budget Growth and Multi-Vendor Expansion Expected to Reshape ACH Fraud Prevention Strategies

Organizations expect a 25% expansion in their ACH fraud prevention vendor base, reflecting broader coverage and use of specialized tools. Budgets are projected to grow 10% annually, though this lags vendor adoption. Willingness to invest shows readiness to diversify providers, but rising costs may drive future consolidation as prevention stacks become increasingly complex and resource-intensive.[1]

1 First Party Fraud Buyer Demand Survey, July 2025 (N=58)

03

Link Index

Friendly ACH Vendor Product Evaluation

Vendor products were evaluated based on their coverage of product capabilities and performance against top solution purchasing criteria

Additional Factors for Consideration

Scalability	Captures the ability to support high transaction volumes and evolving fraud tactics across a growing customer base. Scalable platforms adapt to risk complexity.
Data Quality	Assesses the accuracy of account, transaction, and identity records used to evaluate ACH behavior. High data quality improves dispute resolution outcomes.
Accuracy	Refers to the system's ability to identify intentional ACH reversals while preserving legitimate error resolution. High accuracy minimizes financial loss and customer friction.
Buyer Satisfaction	The extent of buyer satisfaction with a vendor's solution.

● High ◉ Medium ○ Low

1 First Party Fraud Buyer Demand Survey, July 2025 (N=58)

Requirements to Satisfy the Use Case		Buyer Demand for Product Capability[1]
Authenticate Customer Accounts	Verifies that a user accessing a system is the legitimate owner of the account. This typically involves validating identity credentials, such as passwords, multi-factor authentication (MFA), biometric data, or one-time passcodes, at login or during sensitive transactions. The goal is to ensure only authorized users can access or modify account information, protecting against unauthorized access, fraud, and identity theft.	Biometric Authentication ●
		Multi-factor Authentication ●
		App-based Authentication ◉
		Passwordless Authentication ◉
		Continuous Authentication ○
		Mobile Carrier API Access ○
Detect Anomalous Behavioral Activity for Fraud Threats	Analyzes user behavior to identify actions that deviate from typical patterns and may indicate fraudulent intent. By detecting these anomalies in real time, organizations can flag potential first-party, third-party, or synthetic identity fraud before it results in financial loss.	Customer Risk Profiling ●
		Unified Customer View Creation ●
		Behavioral Analytics ◉
		Behavioral Biometrics ◉
		Cross-device Identity Graphing ◉
		Location Intelligence ○
		Mobile Carrier API Access ○
Establish a Customer Identity Profile for Fraud Detection	Aggregates and unifies identity-related data from multiple sources into a single, comprehensive profile for each customer. This includes personal identifiers, account relationships, device usage, behavioral patterns, and historical transactions. The unified profile supports real-time decision-making, improves risk scoring, and reduces false positives in fraud detection systems.	Customer Data Collection & Integration ●
		Data Enrichment ●
		Unified Customer View Creation ●
		Cross-device Identity Graphing ◉
		Identity Resolution ◉
		Cross-Channel Customer Tracking ○
		Fraud Consortium Data Sharing ○
Detect Suspicious Transactions for Fraud	Analyzes transaction data for anomalies, patterns, and behaviors indicative of fraud. This capability involves monitoring transactions in real-time or near-real-time using rule-based engines, machine learning models, or behavioral analytics to flag unusual activity such as sudden changes in spending, high-risk geographies, or rapid movement of funds.	Dispute Pattern Analysis ●
		Fraud Monitoring ●
		Transaction Fraud Risk Scoring ●
		Behavioral Analytics ◉
		Behavioral Biometrics ◉
		ACH Destination Reputation Scoring ○
		Fraud Consortium Data Sharing ○
		Location Intelligence ○

Liminal

Friendly ACH Vendor Product Evaluation

Vendor products were evaluated based on their coverage of product capabilities and performance against top solution purchasing criteria

Additional Factors for Consideration

Scalability	Captures the ability to support high transaction volumes and evolving fraud tactics across a growing customer base. Scalable platforms adapt to risk complexity.
Data Quality	Assesses the accuracy of account, transaction, and identity records used to evaluate ACH behavior. High data quality improves dispute resolution outcomes.
Accuracy	Refers to the system's ability to identify intentional ACH reversals while preserving legitimate error resolution. High accuracy minimizes financial loss and customer friction.
Buyer Satisfaction	The extent of buyer satisfaction with a vendor's solution.

● High ◉ Medium ○ Low

1 First Party Fraud Buyer Demand Survey, July 2025 (N=58)

Requirements to Satisfy the Use Case		Buyer Demand for Product Capability[1]	
Enrich AML Risk Assessments with Transaction Data	Integrates supplementary information, such as geographic location, historical patterns, customer behavior, or third-party intelligence. This enriched data provides deeper insights, enabling more accurate risk assessments and more informed decision-making during transaction monitoring and analysis.	Consumer Financial Transaction Data	◉
Generate a Dynamic User Fraud Risk Score	Calculates a user's likelihood of engaging in fraudulent activity based on both real-time signals and historical behavior. The dynamic nature of the score allows it to evolve with each user interaction, enabling adaptive fraud prevention strategies. This capability helps organizations detect emerging threats, prioritize high-risk users, and apply appropriate controls or interventions.	Customer Risk Profiling	●
		Fraud Monitoring	●
		Transaction Fraud Risk Scoring	●
		Consumer Financial Transaction Data	◉
		Data Enrichment	◉
		Behavioral Analytics	○
		Behavioral Biometrics	○
		Location Intelligence	○
Manage Investigations and Case Workflows	Coordinates the end-to-end process of investigating suspicious activities or incidents. This capability ensures that cases are systematically tracked, documented, and resolved, with clear workflows for assigning tasks, updating statuses, and maintaining records for compliance and audit purposes.	Fraud Alert and Case Management	◉
Document an Audit Trail	Records all actions and changes within a system, providing a detailed log that can be reviewed for compliance, security, and operational transparency. This requirement is essential for tracing the history of transactions, user activities, and system modifications, ensuring accountability and facilitating audits.	Fraud Audit Trail Management	◉

Friendly ACH Vendor Strategy Evaluation

Friendly ACH vendor strategies were assessed based on the top buyer purchasing priorities for the coming years

01

Analytical Capabilities

Denotes the ability to analyze behavioral indicators and payment histories to flag recurring abuse. Advanced analytics improve case prioritization and fraud detection.

02

Automation

Measures the level of automation in flagging suspicious transactions and managing dispute workflows. Automation accelerates detection and reduces operational strain.

03

Compliance Alignment

Evaluates the system's alignment with NACHA rules and internal controls. Compliance-ready tools ensure traceability and regulatory adherence.

04

Adjacent Capabilities

Refers to additional fraud management features that complement friendly ACH fraud prevention, such as identity verification, behavioral analytics, device fingerprinting, or account monitoring.

Friendly ACH Vendor Market Presence Evaluation

The market presence of friendly ACH vendors was evaluated based on company size and growth, leadership perception, funding, digital footprint, and media coverage

Company Size

This criterion measures a vendor's total workforce to indicate its operational capacity, available resources, and scalability. In the identity verification sector, a larger company size often corresponds to greater infrastructure, regulatory expertise, and client support capabilities, reflecting an organization's ability to sustain and evolve its service delivery.

Employee Growth (YoY)

This criterion tracks the year-over-year change in a vendor's workforce, signaling organizational expansion and investment in capability areas such as compliance, technology development, and customer support. Sustained growth can indicate rising demand for solutions and the vendor's capacity to scale operations to meet evolving client requirements.

Market Leadership Perception

This criterion captures how the market perceives a vendor's leadership within the identity verification landscape, including its innovation, reliability, and influence. A strong leadership perception suggests trust in the vendor's solutions, the ability to shape industry standards, and recognition as a preferred partner for compliance and verification initiatives.

Funding History

This criterion assesses the vendor's financial backing, including the volume, frequency, and sources of external investment. A strong funding record demonstrates market confidence, provides resources for innovation and expansion, and supports long-term stability within the identity verification ecosystem.

Digital Footprint

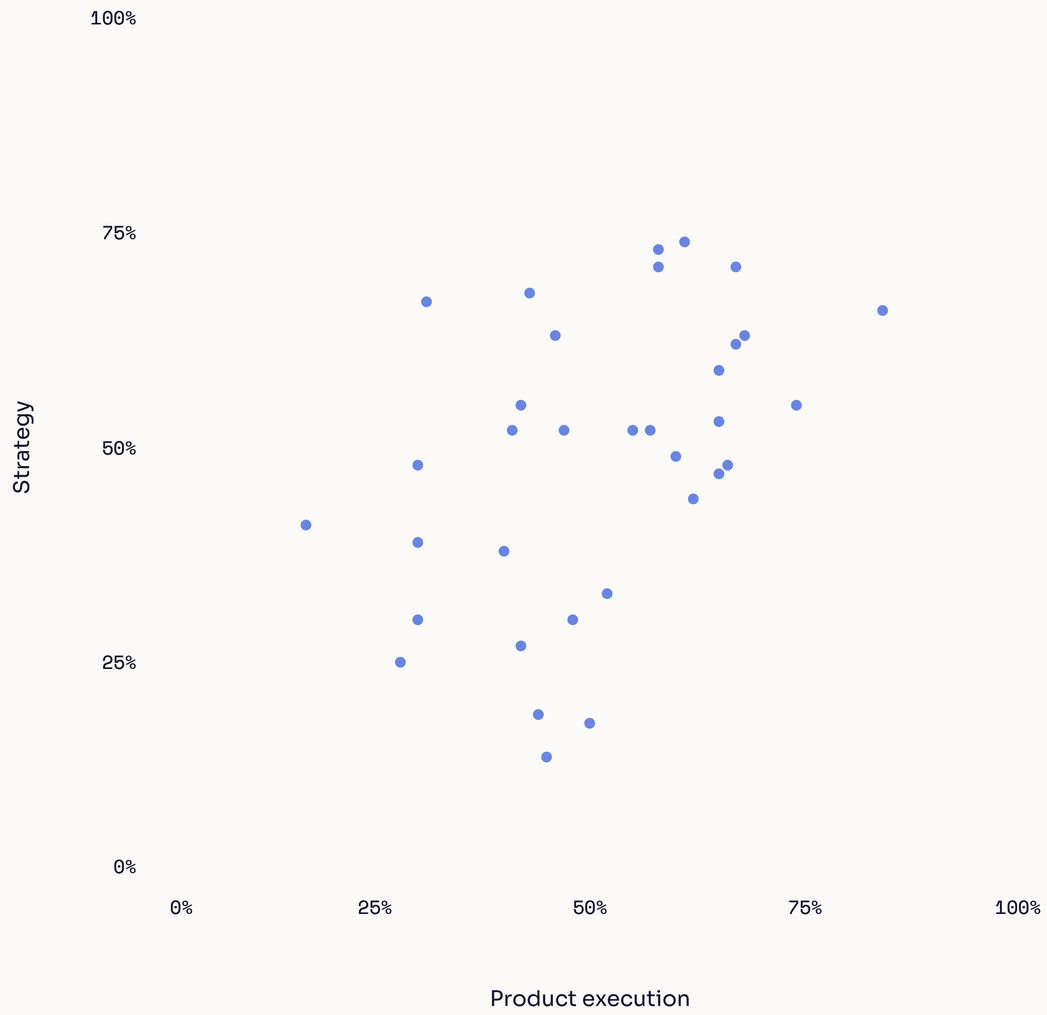
This criterion evaluates the extent and quality of a vendor's digital presence, including its website performance, social engagement, and online visibility. A strong digital footprint indicates active market communication, accessibility to buyers, and transparency about product capabilities and compliance posture.

Media Coverage

This criterion measures the volume and sentiment of media mentions related to the vendor across industry and mainstream sources. Consistent, positive coverage reflects market relevance, public trust, and influence, while high visibility across credible outlets can signal leadership and authority in the identity verification space.

Friendly ACH in Banking: Vendor Evaluation

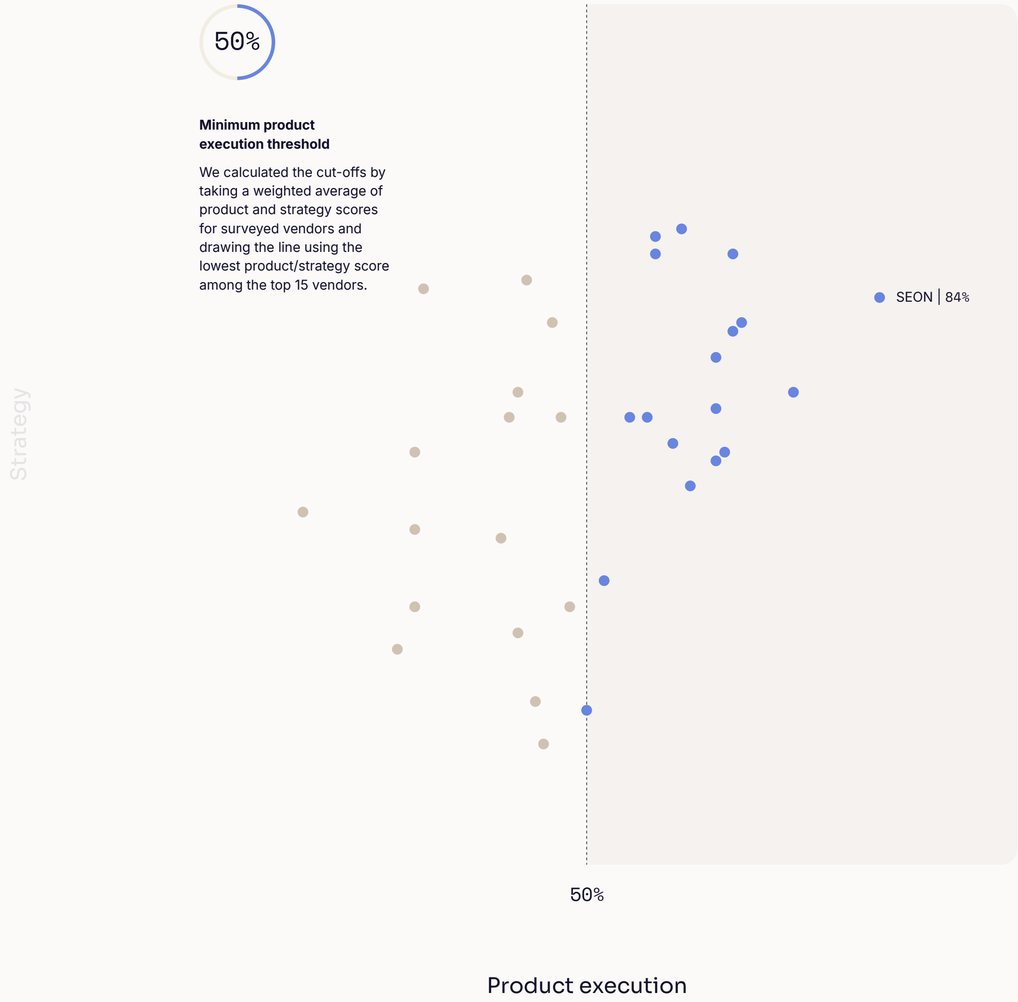
Liminal evaluated 34 vendors that solve the Friendly ACH Fraud in Banking use case. Minimum product execution and strategy thresholds were established to identify the leading vendors



Leadership Thresholds in Friendly ACH

Minimum product execution threshold

To determine the minimum product execution threshold for friendly ACH fraud, Liminal analyzed buyer responses across banking and payments sectors to identify the most valued functional capabilities. These include detection accuracy, scalability, data quality, automation, and integration with real-time return code analysis. Vendors must achieve a minimum product execution score of 50% to meet the operational and compliance requirements expected of leading ACH fraud prevention solutions.



Leadership Thresholds in Friendly ACH

Minimum strategy threshold

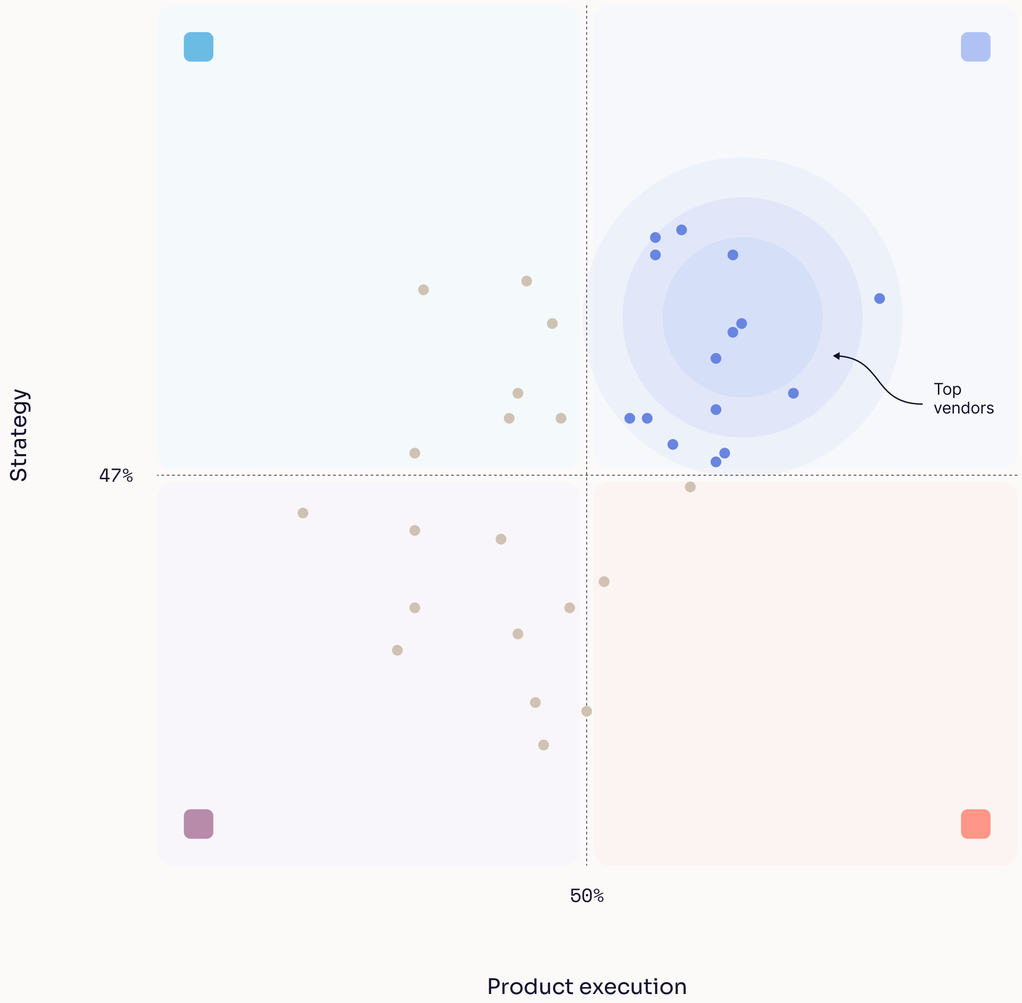
The strategic threshold was defined by assessing future-oriented capabilities that align with market demand for adaptability and transparency. These elements include real-time detection, explainable AI models, automated dispute workflows, and standardized taxonomy integration. Vendors must achieve a minimum strategy score of 47% to demonstrate a proactive, forward-looking approach capable of addressing emerging fraud patterns, regulatory shifts, and operational challenges in ACH fraud management.

Minimum strategy threshold

We calculated the cut-offs by taking a weighted average of product and strategy scores for surveyed vendors and drawing the line using the lowest product/strategy score among the top 15 vendors.

Friendly ACH: Leading Vendors

Among the 34 vendors Liminal evaluated that solve the Friendly ACH Fraud in Banking use case, 15 leading vendors met the minimum product and strategy threshold



Adjacent Vendors
Strong overall solutions but do not have the required capabilities for this use case

Leading Vendors
Strong overall solutions that possess the must have product and strategy capabilities for this use case

Specialized Vendors
Solutions that can solve for a part of the use case but do not have all must have capabilities

Product-Focused Vendors
Solutions with strong product capabilities but do not meet the strategy score threshold

15 Leaders, 34 Evaluated Vendors

Liminal evaluated 34 vendors that solve the Friendly ACH Fraud in Banking use case across the product and strategy criteria, and determined 15 leading vendors

Leader

ACI Worldwide
AppGate
DataVisor
Equifax (Kount)
Feedzai
FICO
Fraud.net
Nasdaq Verafin
NICE Actimize
Outseer
Sardine
SEON
Sift
Unit21
Visa

Other Evaluated Vendors

Adjacent Vendor

Abrigo
DataSeers
Experian
Hawk
LexisNexis Risk Solutions
Plaid
SymphonyAI

Product-Focused

FrankieOne
Socure
Transmit Security

Specialized Vendor

Accertify
Advanced Fraud Solutions
Alloy
Coris
Early Warning
FIS
Flagright
Sonar
TransUnion

Link Index Leading Vendors for Friendly ACH Fraud in Banking in 2025

This view includes the product and strategy score cut-off, showcasing the 15 leading vendors for this year's Friendly ACH Fraud in Banking Index

Market Presence

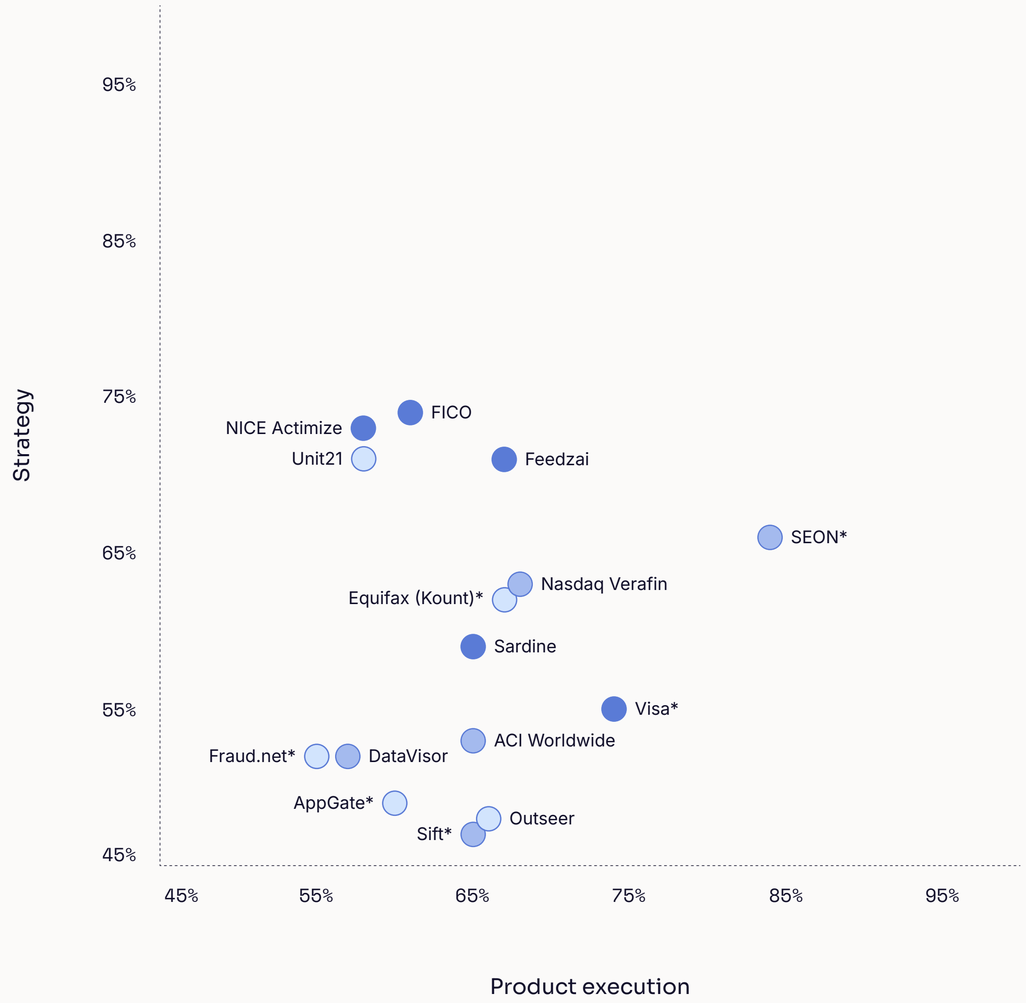
- Exceptional
- Excellent
- Strong

Inclusion Cutoff

Product Score 50%
Strategy Score 47%

We calculated the cut-offs by taking a weighted average of product and strategy scores for surveyed vendors and drawing the line using the lowest product/strategy score among the top 15 vendors.

Companies with an asterisk (*) participated in an Analyst Briefing with Liminal for this report.



Friendly ACH Leading Vendor Characteristics

Friendly ACH vendors take distinct approaches based on detection sophistication, data integration, and risk management needs

End-to-End Fraud and AML Platforms

These vendors deliver comprehensive solutions that integrate ACH fraud prevention within broader anti-fraud and compliance frameworks. They provide real-time transaction monitoring, behavioral analytics, risk scoring, and AML compliance tools that detect anomalous activity across payment channels. Typically serving banks and large financial institutions, these platforms combine fraud detection, KYC, and transaction risk management to deliver unified oversight and regulatory alignment.

Fraud Detection and Risk Analytics Platforms

These platforms specialize in identifying first-party and friendly ACH fraud through adaptive analytics, hybrid detection models, and data enrichment. Leveraging machine learning, behavioral biometrics, and real-time return code analysis, they detect patterns indicative of fraudulent disputes or abuse of ACH dispute mechanisms. Designed for scalability and integration, these platforms serve mid-sized institutions seeking strong detection capabilities without full AML infrastructure.

Authentication and Identity Intelligence Providers

These vendors focus on strengthening authentication and user verification within ACH ecosystems. Their tools include biometric authentication, multi-factor authentication (MFA), and device or behavioral profiling to verify legitimate account holders and reduce unauthorized access. Many also integrate with fraud monitoring systems to enhance accuracy and prevent friendly fraud at the point of transaction initiation or dispute filing.

Specialized ACH Dispute and Workflow Solutions

These vendors target dispute management and case resolution, providing automation and audit-trail capabilities for ACH returns and reversals. Their systems streamline investigation workflows, unify transaction and customer data, and ensure compliance with NACHA regulations. Ideal for institutions handling high dispute volumes, these solutions improve efficiency, data quality, and traceability while reducing operational strain associated with manual reviews.

Friendly ACH Leading Vendor Future Outlook

Leading vendors are shaping the future of friendly ACH fraud prevention through real-time detection, standardized data integration, and adaptive fraud intelligence

01

Real-time, Automated Detection

Leading vendors are prioritizing real-time monitoring and alerting to detect fraudulent ACH activity before funds are transferred. Their systems analyze transaction patterns, dispute histories, and behavioral indicators as data is received, allowing institutions to intervene instantly. By automating detection and reducing reliance on manual review, these vendors improve operational capability and limit financial exposure to friendly fraud disputes.

02

Standardized Data Integration and Return Code Analysis

Top vendors are embedding NACHA return codes and metadata directly into fraud detection workflows to strengthen classification and transparency. Standardized taxonomies and integrated dashboards improve cross-institution collaboration and benchmarking. This approach allows fraud teams to operationalize return code data, reducing classification mismatches and simplifying compliance reporting.

03

Adaptive Fraud Intelligence and Behavioral Analytics

Vendors are deploying hybrid fraud detection models that combine rules-based and AI/ML analytics to adapt to evolving first-party fraud tactics. These systems analyze customer behavior, transaction context, and device intelligence to generate dynamic risk scores. By integrating behavioral biometrics, customer profiling, and contextual data, they enhance detection accuracy while reducing false positives.

04

Workflow Automation and Dispute Management

Modern solutions now include automated case management and audit-trail functionality to simplify dispute resolution. These platforms consolidate transaction data, documentation, and investigation records into unified dashboards, ensuring compliance with NACHA requirements and institutional audit policies. Automation reduces manual workload, shortens resolution times, and strengthens accountability throughout the ACH dispute process.

04

Vendor Overviews

Unit21

About Unit21

Unit21 enables risk and compliance teams to prevent friendly ACH fraud and other first-party threats through a configurable, no-code platform that supports real-time decisioning across transactions, instruments, and entities. The system inspects sender and receiver behavior longitudinally, detects anomalies, and surfaces hidden relationships using graph-based link analysis. Rules can incorporate device intelligence (e.g., jailbreak status, VPN use) and external risk signals, and apply sequential logic to capture patterns like “A-then-B-then-C” common in coordinated abuse.

Company Information (as of September 2025)

Headquarters	San Francisco, California
No. of Employees	97
Last Raised	$45 M Series C, June 2023
Market Cap	–
Industry Focus	Financial Services
Geographic Focus	North America, Europe, Asia Pacific, LATAM
Notable Customers	greendot bank, sallie mae, AMERICA FIRST CREDIT UNION

Performance on Friendly ACH Link Index Benchmarking Criteria

Avg.	Criteria		Performance[1]
Strategy	**Analytical Capabilities**	The solution’s ability to process, interpret, and generate insights from data.	Excellent
	Automation	The solution’s ability to streamline tasks and reduce effort.	Excellent
	Compliance Alignment	The solution’s adherence to regulatory, industry, and organizational standards.	Exceptional
	Adjacent Capabilities	The solution’s complementary features that extend beyond core functionality.	Exceptional
Product	**Product Capability**	The solution’s range of features and functionalities.	Exceptional
	Scalability	The solution’s ability to maintain performance at high volumes.	Excellent
	Data Quality	The completeness, accuracy, and timeliness of data.	Exceptional
	Accuracy	The solution’s precision in performing its intended function.	Exceptional
	Buyer Satisfaction	The solution’s satisfaction rating among practitioners.	Strong
Market Presence	**Company Size**	Total employee headcount.	Strong
	Employee Growth	Year over year employee growth.	Strong
	Market Leadership	The solution’s perceived leadership in the market.	Strong
	Funding	The company’s total capital raised through investments.	Excellent
	Digital Footprint	The company’s online presence across web and social platforms.	Strong
	Media Coverage	The company’s visibility in industry and general press.	Excellent

Exceptional Excellent Strong

1 The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of only the leading vendor for Friendly ACH in Banking. Vendors outside the scoring buckets are not considered leading vendors for Friendly ACH in Banking.

Unit21

Analyst Notes

For friendly ACH fraud prevention, Unit21 focuses on first-party fraud patterns across transaction, instrument, and entity levels, applying directional monitoring to senders and receivers. It supports batch files, a near-real-time API that posts every 10 minutes, and a real-time API that returns decisions in approximately 250 milliseconds.[1] Graph-based rules and network analysis detect clusters sharing personally identifiable information (PII), devices, or IPs to identify multi-account schemes and bonus abuse. Device intelligence from Fingerprint adds jailbreak status, VPN use, and browser tampering indicators for higher-confidence interdiction. Rules also draw on non-transactional events, such as login attempts, profile changes, and the disablement of two-factor authentication (2FA) to add friction for high-risk accounts.[1] Validation tools test rule configurations on historical data or in shadow mode before activation, and the platform tracks alert volumes and false positives to fine-tune thresholds over time.

The strategy centers on a self-service rule engine that operations teams can modify without code, supported by rapid validation to reduce false positives and confirm business fit. Continued investment targets sub-250-millisecond real-time screening and live event sequencing so rules can capture “A-then-B-then-C” activity patterns common in friendly ACH fraud.[1] AI agents now handle structured alert triage with consistent, auditable steps. In contrast, customer-defined agents and auto-disposition are planned for summer 2025.[1] Upcoming enhancements include rule recommendations and broader AI assistance for testing and screening. Partnerships that supply device intelligence enrich the risk context without requiring on-premises deployment.

Unit21’s platform is used by fintechs for real-time prevention and by traditional banks via batch or standard APIs, which are aligned with their legacy cores. Its consortium includes over 80 banks, credit unions, and fintechs representing about 34% of the U.S. adult population.[1] Integrated into the rule engine, the consortium enables participants to screen applicants and customers against peer-reported fraud. The same graph and device features support adjacent trust-and-safety use cases such as promotional abuse, while the primary focus remains on financial services and ACH fraud defense.

● High ◉ Medium ○ Low

1 Liminal Analyst Briefing
2 Greyed out capabilities are not offered with the vendor solution.
3 First Party Fraud Buyer Demand Survey, July 2025 (N=58)

Friendly ACH Capabilities[2]

Requirements to Satisfy the Use Case		Buyer Demand for Product Capability[3]
Authenticate Customer Accounts	Verifies that a user accessing a system is the legitimate owner of the account. This typically involves validating identity credentials, such as passwords, multi-factor authentication (MFA), biometric data, or one-time passcodes, at login or during sensitive transactions. The goal is to ensure only authorized users can access or modify account information, protecting against unauthorized access, fraud, and identity theft.	Biometric Authentication ○ Multi-factor Authentication ○ App-based Authentication ◉ Passwordless Authentication ◉ Continuous Authentication ○ Mobile Carrier API Access ○
Detect Anomalous Behavioral Activity for Fraud Threats	Analyzes user behavior to identify actions that deviate from typical patterns and may indicate fraudulent intent. By detecting these anomalies in real time, organizations can flag potential first-party, third-party, or synthetic identity fraud before it results in financial loss.	Customer Risk Profiling ● Unified Customer View Creation ● Behavioral Analytics ◉ Behavioral Biometrics ◉ Cross-device Identity Graphing ◉ Location Intelligence ○ Mobile Carrier API Access ○
Establish a Customer Identity Profile for Fraud Detection	Aggregates and unifies identity-related data from multiple sources into a single, comprehensive profile for each customer. This includes personal identifiers, account relationships, device usage, behavioral patterns, and historical transactions. The unified profile supports real-time decision-making, improves risk scoring, and reduces false positives in fraud detection systems.	Customer Data Collection & Integration ● Data Enrichment ● Unified Customer View Creation ● Cross-device Identity Graphing ◉ Identity Resolution ◉ Cross-Channel Customer Tracking ○ Fraud Consortium Data Sharing ○
Detect Suspicious Transactions for Fraud	Analyzes transaction data for anomalies, patterns, and behaviors indicative of fraud. This capability involves monitoring transactions in real-time or near-real-time using rule-based engines, machine learning models, or behavioral analytics to flag unusual activity such as sudden changes in spending, high-risk geographies, or rapid movement of funds.	Dispute Pattern Analysis ● Fraud Monitoring ● Transaction Fraud Risk Scoring ● Behavioral Analytics ◉ Behavioral Biometrics ◉ ACH Destination Reputation Scoring ○ Fraud Consortium Data Sharing ○ Location Intelligence ○

Unit21

Analyst Notes

For friendly ACH fraud prevention, Unit21 focuses on first-party fraud patterns across transaction, instrument, and entity levels, applying directional monitoring to senders and receivers. It supports batch files, a near-real-time API that posts every 10 minutes, and a real-time API that returns decisions in approximately 250 milliseconds.[1] Graph-based rules and network analysis detect clusters sharing personally identifiable information (PII), devices, or IPs to identify multi-account schemes and bonus abuse. Device intelligence from Fingerprint adds jailbreak status, VPN use, and browser tampering indicators for higher-confidence interdiction. Rules also draw on non-transactional events, such as login attempts, profile changes, and the disablement of two-factor authentication (2FA) to add friction for high-risk accounts.[1] Validation tools test rule configurations on historical data or in shadow mode before activation, and the platform tracks alert volumes and false positives to fine-tune thresholds over time.

The strategy centers on a self-service rule engine that operations teams can modify without code, supported by rapid validation to reduce false positives and confirm business fit. Continued investment targets sub-250-millisecond real-time screening and live event sequencing so rules can capture "A-then-B-then-C" activity patterns common in friendly ACH fraud.[1] AI agents now handle structured alert triage with consistent, auditable steps. In contrast, customer-defined agents and auto-disposition are planned for summer 2025.[1] Upcoming enhancements include rule recommendations and broader AI assistance for testing and screening. Partnerships that supply device intelligence enrich the risk context without requiring on-premises deployment.

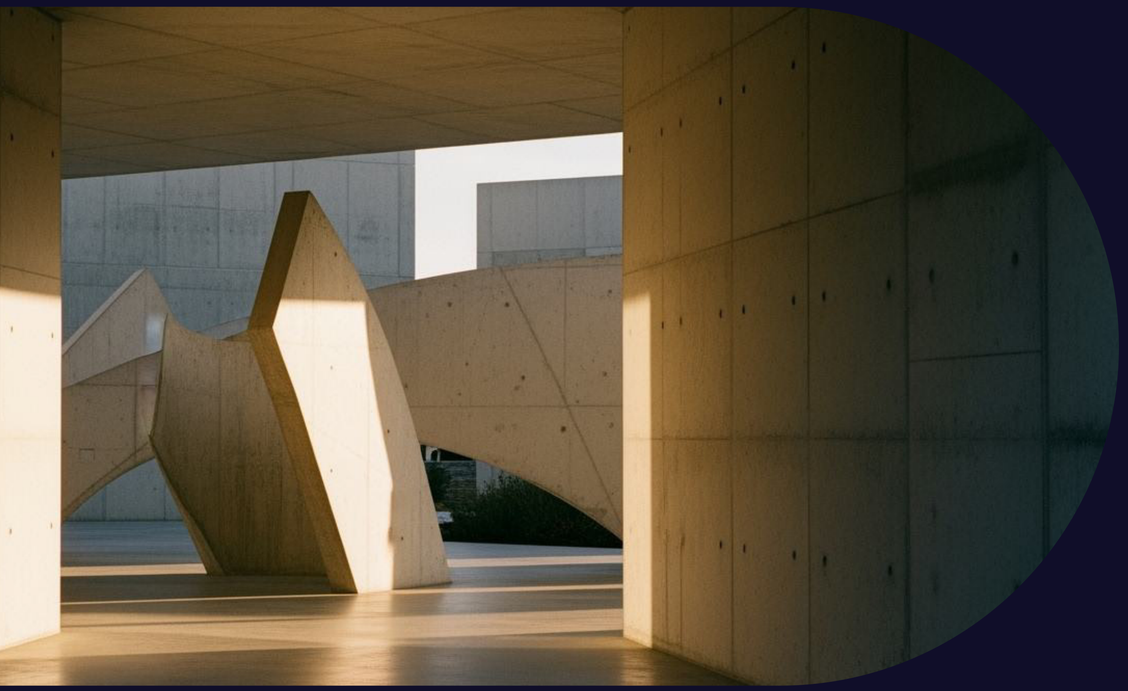
Unit21's platform is used by fintechs for real-time prevention and by traditional banks via batch or standard APIs, which are aligned with their legacy cores. Its consortium includes over 80 banks, credit unions, and fintechs representing about 34% of the U.S. adult population.[1] Integrated into the rule engine, the consortium enables participants to screen applicants and customers against peer-reported fraud. The same graph and device features support adjacent trust-and-safety use cases such as promotional abuse, while the primary focus remains on financial services and ACH fraud defense.

Friendly ACH Capabilities[2]

Requirements to Satisfy the Use Case		Buyer Demand for Product Capability[3]	
Enrich AML Risk Assessments with Transaction Data	Integrates supplementary information, such as geographic location, historical patterns, customer behavior, or third-party intelligence. This enriched data provides deeper insights, enabling more accurate risk assessments and more informed decision-making during transaction monitoring and analysis.	Consumer Financial Transaction Data	◉
Generate a Dynamic User Fraud Risk Score	Calculates a user's likelihood of engaging in fraudulent activity based on both real-time signals and historical behavior. The dynamic nature of the score allows it to evolve with each user interaction, enabling adaptive fraud prevention strategies. This capability helps organizations detect emerging threats, prioritize high-risk users, and apply appropriate controls or interventions.	Customer Risk Profiling	●
		Fraud Monitoring	●
		Transaction Fraud Risk Scoring	●
		Consumer Financial Transaction Data	◉
		Data Enrichment	◉
		Behavioral Analytics	○
		Behavioral Biometrics	○
		Location Intelligence	○
Manage Investigations and Case Workflows	Coordinates the end-to-end process of investigating suspicious activities or incidents. This capability ensures that cases are systematically tracked, documented, and resolved, with clear workflows for assigning tasks, updating statuses, and maintaining records for compliance and audit purposes.	Fraud Alert and Case Management	◉
Document an Audit Trail	Records all actions and changes within a system, providing a detailed log that can be reviewed for compliance, security, and operational transparency. This requirement is essential for tracing the history of transactions, user activities, and system modifications, ensuring accountability and facilitating audits.	Fraud Audit Trail Management	◉

● High ◉ Medium ○ Low

1 Liminal Analyst Briefing
2 Greyed out capabilities are not offered with the vendor solution.
3 First Party Fraud Buyer Demand Survey, July 2025 (N=58)



05

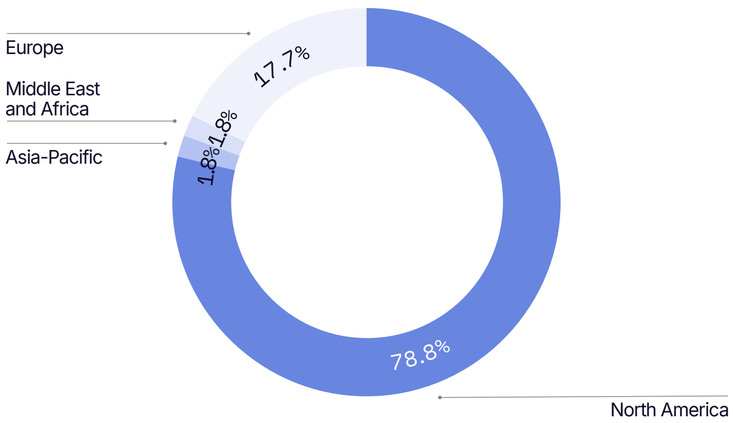
Appendix

Market Presence Survey Demographics

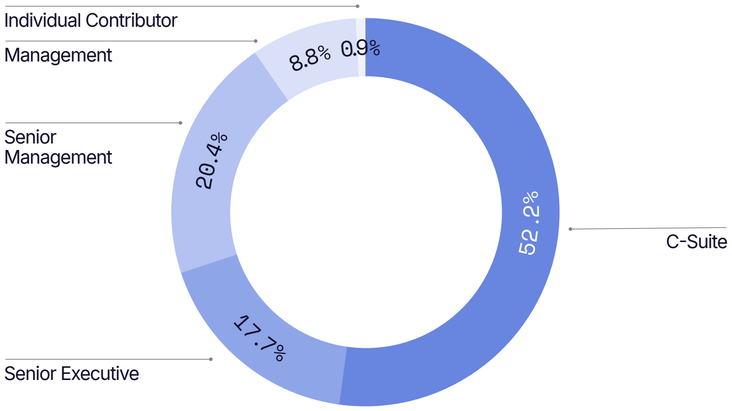
Survey Respondent Demongraphics (N=113)[1]

Geography

By Region, highest priority based on revenue

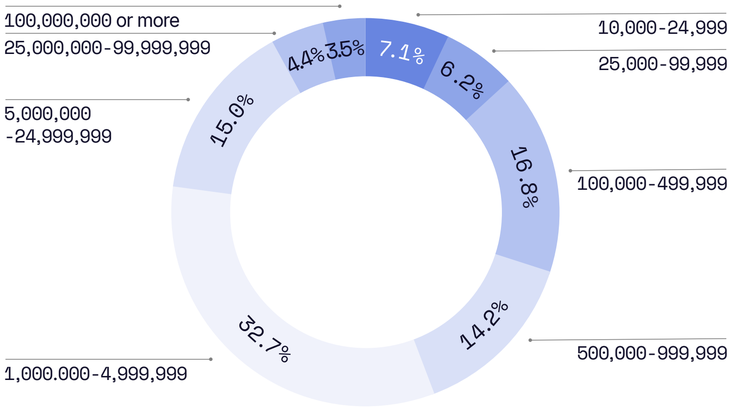


Job Level



Company Size

By Customers



1 First Party Fraud Buyer Demand Survey, July 2025 (N=113)

Link Index Methodology

Exceptional, Excellent, Strong Scoring Buckets Definitions

Scoring Buckets	Definition
Exceptional	Vendors in this category demonstrate the highest level of capability in addressing friendly ACH fraud, ranking above the third quartile among leading providers. These vendors go beyond standard fraud detection by leveraging advanced behavioral analytics, payment pattern recognition, and AI-driven dispute resolution. Their platforms enable financial institutions to accurately distinguish between genuine errors and fraudulent reversals, reduce operational losses, and maintain compliance with evolving ACH dispute regulations.
Excellent	Vendors in this category provide highly effective solutions for mitigating friendly ACH fraud, ranking between the first and third quartile among leading providers. They deliver strong detection tools, reliable dispute management workflows, and scalable automation, though they may not reach the same refinement as Exceptional vendors. Their platforms improve reversal claim accuracy, strengthen fraud risk assessment, and support compliance reporting, making them a strong choice for institutions seeking effective and cost-conscious protection against ACH abuse.
Strong	Vendors in this category meet the core requirements for handling friendly ACH fraud, ranking below the first quartile among top providers while still outperforming those not making the final list. They offer dependable detection and dispute resolution tools that cover fundamental compliance and risk management needs. While they may not provide advanced automation, deep integrations, or AI-driven behavioral analysis, their offerings remain suitable for organizations requiring essential protection against ACH reversals and disputes.

Product Capability Definitions

Capability	Definition
ACH Destination Reputation Scoring	ACH Destination Reputation Scoring is a risk assessment capability that evaluates the trustworthiness of recipient bank accounts in ACH (Automated Clearing House) transactions. It assigns a dynamic score to destination accounts based on historical transaction behavior, known associations with fraud, and risk signals across the payment network. This scoring helps financial institutions and payment processors flag suspicious or high-risk transfers before funds are disbursed.
App-based Authentication	App-based authentication, such as the use of an authenticator app, is a method that provides an additional layer of security for online accounts through multi-factor authentication (MFA). These apps generate time-based, one-time passcodes (TOTP or OTP) on a user's smartphone, which must be entered in addition to the usual login credentials (like a password) to gain access to an account.
Behavioral Analytics	Behavioral analytics is a data analysis process that focuses on understanding how users interact with systems and applications to detect unusual behaviors that may indicate security threats or unauthorized activities. It tracks and analyzes a wide range of user activities - from account creation and form submissions to purchasing behavior - to glean insights into user preferences, habits, and intentions.
Behavioral Biometrics	Behavioral biometrics identifies individuals based on their unique patterns of behavior, particularly in the context of human-computer interaction. Unlike physical biometrics, which rely on innate physical characteristics like fingerprints or iris patterns, behavioral biometrics focuses on patterns that emerge from a person's natural interactions and activities, such as typing rhythm, mouse movements, gait, and voice dynamics.
Biometric Authentication	Biometric authentication refers to a process that verifies a user’s identity using their unique biological traits such as fingerprints, voices, retinas, and facial features. Biometric authentication can use both physical biometrics (based on physiological features) and behavioral biometrics (based on how people behave).
Consumer Financial Transaction Data	Consumer financial transaction data refers to the detailed personal financial information collected from various financial institutions, including transaction history, balance details, and fee information related to credit cards, loans, mortgages, and securities. It encompasses purchases, payments, debits, credits, interest payments, and other consumer transactions.

Product Capability Definitions

Capability	Definition
Continuous Authentication	Continuous authentication is a security approach that verifies a user's identity continuously throughout a session, rather than just at the point of login.
Cross-Channel Customer Tracking	Cross-channel or omnichannel tracking is the process of monitoring and analyzing a user's interactions and behaviors across multiple communication channels, such as email, social media, websites, mobile apps, and in-store visits. This capability involves collecting and integrating data from various touchpoints to create a unified view of the customer journey.
Cross-Device Identity Graphing	Cross-device identity graphing is the process of linking and mapping user identities across multiple devices to create a unified, cohesive profile. This capability leverages probabilistic and deterministic data matching techniques to accurately consolidate user interactions from different devices into a single identity graph.
Customer Data Collection & Integration	Data collection and integration is the process of gathering data from various sources and combining it into a unified system for analysis and use. It helps organizations create comprehensive customer profiles and streamline data management.
Customer Risk Profiling	Customer risk profiling is the process of evaluating and categorizing customers based on their likelihood of exhibiting high-risk behavior, such as fraud, credit default, policy abuse, or non-compliance. This involves analyzing data points such as identity attributes, transaction history, behavioral patterns, device and location signals, and external risk indicators to assign a risk score or classification.
Data Enrichment	Data enrichment is the process of appending or otherwise enhancing first-party data with relevant context from additional internal or external sources. It involves collecting and consolidating data from various sources, such as social media, customer relationship management (CRM) systems, and customer data platforms (CDPs), and then using machine learning algorithms and other techniques to enhance the data's accuracy, completeness, and relevance.

Product Capability Definitions

Capability	Definition
Dispute Pattern Analysis	Examines historical and real-time dispute data, such as chargebacks, returns, or refund claims, to identify recurring behaviors, anomalies, or fraud signals. It helps organizations uncover trends related to specific customers, products, payment methods, or transaction types. This analysis is used to distinguish between legitimate customer issues and potential abuse, such as friendly fraud or coordinated attacks.
Fraud Alert and Case Management	Fraud alert and case management detects suspicious activity in real-time, generating alerts, and managing investigation workflows to determine whether fraud has occurred. It enables organizations to triage, escalate, and resolve alerts efficiently while maintaining detailed audit trails and cross-functional collaboration.
Fraud Audit Trail Management	Fraud Audit Trail Management is a product capability that records, tracks, and preserves all actions, decisions, and system events related to fraud detection and investigation. It provides a transparent, time-stamped history of activities for compliance, internal review, and legal defensibility.
Fraud Consortium Data Sharing	Fraud Consortium Data Sharing is a collaborative model where organizations share fraud-related intelligence—such as suspicious identities, behaviors, devices, or transaction patterns—to improve collective detection and prevention capabilities. By pooling anonymized or pseudonymized data, consortium members gain broader visibility into emerging fraud tactics that may not be apparent within their own systems. This shared approach helps reduce blind spots, catch repeat offenders across platforms, and strengthen defenses against sophisticated fraud rings.
Fraud Monitoring	Fraud monitoring is the surveillance and analysis of networks, accounts, and transactions to identify potentially fraudulent activity for automated fraud decisioning.
Identity Resolution	Identity resolution is the process of accurately linking multiple identifiers and data points across different devices, channels, and interactions to create a unified, cohesive view of an individual.

Product Capability Definitions

Capability	Definition
Location Intelligence	Location intelligence leverages geolocation data to understand user behavior, deliver personalized services, and enhance marketing strategies based on real-time location information.
Mobile Carrier API Access	Mobile Carrier API Access refers to the ability to integrate and utilize APIs provided by mobile network operators (MNOs) to access mobile subscriber data and services, such as authentication, identity verification, and SIM swap detection.
Multi-Factor Authentication	Multi-factor Authentication (MFA) is a security process that requires users to provide two or more verification factors to gain access to a resource such as an application, online account, or VPN. It enhances security by combining multiple methods of authentication, reducing the risk of unauthorized access.
Passwordless Authentication	Passwordless authentication is a security process that allows users to access their accounts without the need for a traditional password. Instead, it uses alternative methods such as biometrics, email or SMS codes, or hardware tokens to verify the user's identity.
Transaction Fraud Risk Scoring	Assigns a risk score to a financial transaction based on its likelihood of being fraudulent. The score is calculated using various factors such as transaction amount, frequency, location, and user behavior, and it helps determine whether to approve, decline, or further investigate the transaction. The scoring model may utilize rule-based methods, AI-based models, or a combination of both to detect suspicious activities.
Unified Customer View Creation	Unified customer view creation is the process of consolidating data from multiple sources to create a single, comprehensive profile for each customer. It enables organizations to gain a holistic understanding of their customers, enhancing personalization and improving decision-making.

Link Index Methodology

Product

Product Criteria	Weighting	Definition	Why It Matters
Friendly ACH Capabilities	60.00%	The breadth of capabilities a vendor offers to address the requirements of this use case.	Determines how comprehensively a vendor can detect, prevent, and resolve friendly ACH fraud incidents.
Scalability	10.00%	Captures the ability to support high transaction volumes and evolving fraud tactics across a growing customer base. Scalable platforms adapt to risk complexity.	Ensures solutions remain effective as transaction volumes and fraud sophistication increase.
Data Quality	10.00%	Assesses the accuracy of account, transaction, and identity records used to evaluate ACH behavior. High data quality improves dispute resolution outcomes.	High-quality data strengthens fraud detection and reduces false disputes in ACH transactions.
Accuracy	5.00%	Refers to the system's ability to identify intentional ACH reversals while preserving legitimate error resolution. High accuracy minimizes financial loss and customer friction.	Precision in identifying fraudulent reversals limits revenue loss and maintains customer trust.
Buyer Satisfaction	15.00%	The extent of buyer satisfaction with a vendor's solution.	Reflects real-world effectiveness and confidence in the solution's performance against friendly ACH fraud.

Link Index Methodology

Strategy

Strategy Criteria	Weighting	Definition	Why It Matters
Analytical Capabilities	27.00%	Denotes the ability to analyze behavioral indicators and payment histories to flag recurring abuse. Advanced analytics improve case prioritization and fraud detection.	Strong analytics enable earlier detection of friendly ACH abuse and improve investigative accuracy.
Automation	27.00%	Measures the level of automation in flagging suspicious transactions and managing dispute workflows. Automation accelerates detection and reduces operational strain.	Automation improves operational efficiency and allows faster resolution of fraudulent ACH claims.
Compliance Alignment	27.00%	Evaluates the system's alignment with NACHA rules and internal controls. Compliance-ready tools ensure traceability and regulatory adherence.	Ensures fraud management processes meet NACHA and internal governance standards, reducing compliance risk.
Adjacent Capabilities	19.00%	Refers to additional fraud management features that complement friendly ACH fraud prevention, such as identity verification, behavioral analytics, device fingerprinting, or account monitoring.	Broad adjacent capabilities strengthen overall fraud prevention by addressing related risks beyond ACH reversals.

Link Index Methodology

Market Presence

Market Criteria	Weighting	Definition	Why It Matters
Company Size	20.00%	The total employee headcount of a company.	A larger workforce often indicates greater operational capacity, enabling sustained product development and customer support.
Employee Growth (YoY)	20.00%	How fast a company's employee count is growing.	Rapid employee growth signals business expansion and investment in capability building, reflecting overall organizational momentum.
Market Leadership Perception	20.00%	The number of buyers who believe this vendor is a market leader.	Strong market perception enhances credibility and buyer confidence, influencing vendor selection and partnership opportunities.
Funding History	30.00%	Total funding a company has incurred.	Adequate funding supports long-term stability, innovation, and scalability, ensuring the vendor can sustain product improvement and client needs.
Digital Footprint	5.00%	The company’s total social media footprint.	A strong online presence increases visibility, engagement, and perceived relevance in the chargeback prevention market.
Media Coverage	5.00%	Vendor mentions/quotes in authoritative outlets reflect market presence.	Frequent and credible media mentions demonstrate thought leadership, validate market influence, and reinforce trust among prospective buyers.

Liminal™

From Research to Revenue - The Actionable Intelligence Platform

The same depth and rigor you've just read, now powering your real-time link between strategy and execution

Unify market, competitor, and buyer intelligence to power every motion - from sales execution to product strategy. With Liminal, your GTM team will always know where to play and how to win.

Discover

map vendors, products, and use-cases to reveal actionable whitespace, monitor in real-time

Position

target with precision: 35k+ personas continuously refreshed with in-market buyer intelligence

Mobilize

connect deeply, quickly, and at scale with dynamic battlecards and personalized prospect outreach

Execute

close faster and win more with deal-level insights embedded across your workflow

GTM teams using Liminal **close more deals**

Proven across our portfolio

30%

higher win rates

See how Liminal elevates research into results - actionable intelligence from discovery to close.

Book a Demo

Liminal™

link Index™ Report

Liminal Strategy, Inc.
825 Third Avenue, Suite 1700, New York, NY 10022

www.liminal.co | info@liminal.co