galileo

Fighting Fire with Fire: How to Stop Identity and First-Party Fraud, Romance Scams, Elder Fraud, and Beyond

The Financial Services, Fintech and Brand Fraud Playbook for Stopping Digital Criminal Networks

Here's the reality every financial services organization, fintech and brand faces today: Fraudsters are launching AI-powered attacks faster than most systems can adapt.

While organizations debate implementation timelines, criminals are already using AI and machine learning to bypass legacy fraud detection in real-time. Effective fraud prevention today requires organizations to match criminals' technological sophistication.

Put simply, it requires fighting fire with fire.

According to the Javelin 2025 Identity Fraud Study, identity fraud costs rose sharply in 2024, with total losses in the U.S. amounting to slightly more than $27 billion—a staggering 19% increase from $22.8 billion in 2023.

What makes this surge particularly alarming is its breadth: all fraud types tracked by Javelin increased in losses. Account takeover (ATO), an enduring favorite of fraudsters, had the largest increase, from $12.7 billion in 2023 to nearly $16 billion in 2024

Fraudsters are moving faster and at a greater scale, outsmarting old defenses and leaving many organizations scrambling to keep pace.

This guide is for financial institutions, fintechs, and brands ready to elevate their fraud strategy, turning fraud management from a defensive stance into a proactive, customer-centric approach that drives long-term stability, security, and growth.

Online payment fraud losses are projected to exceed $362 billion in the next five years—and it's getting harder and more expensive to fight fraud that drives those losses.

Putting your Team on Offense: The Escalating Financial Fraud Wars

Effective fraud mitigation is more than loss prevention—it underpins customer trust and long-term growth. Success requires a tailored, data-driven blend of technology, analytics, and expertise.

Each sophisticated attack and emerging scam technique underscores the relentless nature of this challenge, with criminals leveraging AI and machine learning, while exploiting vulnerabilities faster than many organizations can respond.

The surge in account takeover fraud is indicative of a much larger systemic problem. Criminals target a wide variety of accounts—including checking and credit accounts, email, digital wallets, mobile phones, and social media.

Lax authentication standards, like optional multifactor authentication or permissive password policies, have boosted the boom in ATO fraud.

Cybercriminals are not only successfully evading detection by consumers when committing mass amounts of unauthorized takeovers of both financial and non-financial accounts, but also the proprietors of those accounts.

This environment demands that banks and credit unions, fintechs, and brands fundamentally rethink their approach to fraud prevention. The stakes have never been higher, and the cost of inaction continues to rise with each passing quarter.

CHAPTER 1

Why AI is Essential for your Fraud Fighting Strategies

Fraud today requires more than a "one-size-fits-all" approach; layered, adaptable defenses are essential. The era of static rule-based systems has passed, replaced by dynamic, intelligent solutions that evolve alongside emerging threats.

Stay ahead by deploying AI and machine learning to identify new fraud patterns such as synthetic ID creation, elder abuse schemes, first-party fraud manipulation, and constantly evolving scams that traditional systems miss.

It's also critical to protect the customer experience by minimizing false positives so legitimate customers enjoy fast, secure onboarding and transactions. AI-powered fraud detection is essential to achieve this balance.

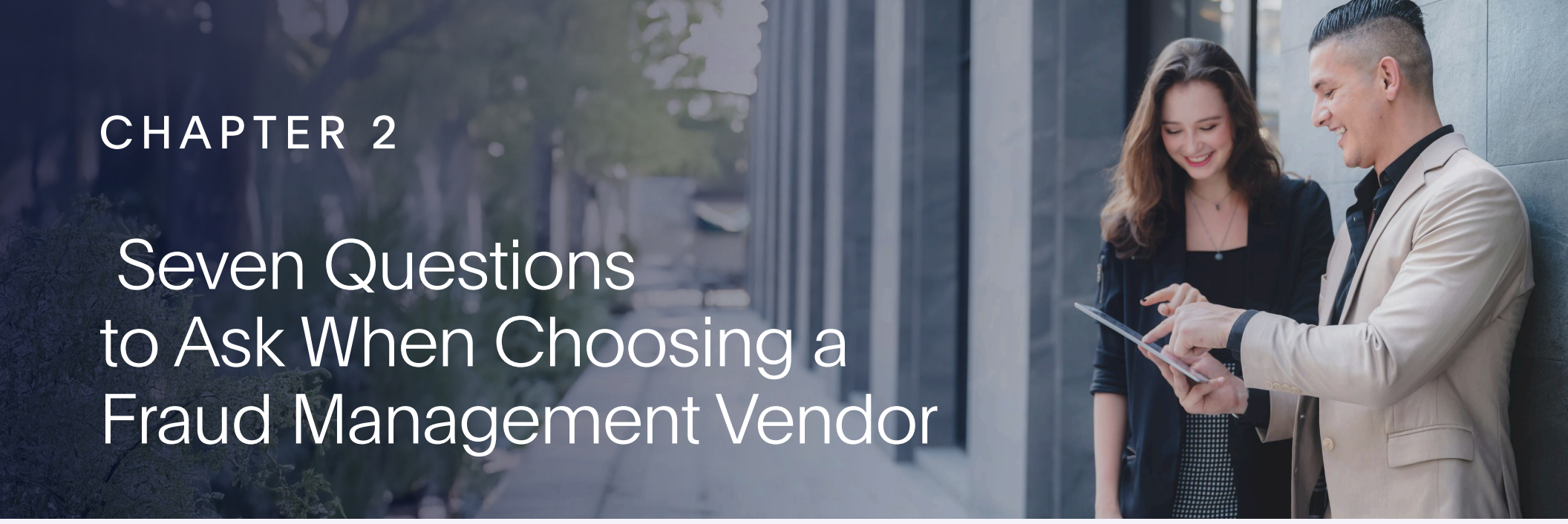
Javelin's research shows consumers who have a working knowledge of artificial intelligence are more supportive of their financial institutions using AI to protect their accounts and identities.

Though just under half (47%) of consumers feel generally knowledgeable about AI and how it works, 81% of those consumers are overwhelmingly comfortable with their FI using AI for account security and fraud protection.

This consumer acceptance is critical as banks begin incorporating more AI into their fraud mitigation strategies and identity verification and authentication practices. Financial institutions are among the most trusted entities by consumers, and part of building and maintaining that trust is ensuring consumers understand what their financial provider is doing to protect them.

AI-enabled fraud strategies can achieve:

- Real-time identification of synthetic ID fraud, elder abuse, and evolving scams
- Seamless customer experience with minimal false positives
- Balanced real-time and post-transaction monitoring
- Analysis of millions of unique spending patterns and transaction behaviors in real time.



CHAPTER 2

Seven Questions to Ask When Choosing a Fraud Management Vendor

A strong fraud partner must be able to help you fight back with the same technology and tools that fraudsters are putting to use. This means deploying the latest advances in AI and machine learning to reduce risk, losses, and operational expenses while protecting customers. When improving your fraud outcomes, you need a partner with deep expertise that balances strong fraud protection with seamless customer experience—supporting confidence, compliance, and operational efficiency at scale.

AI/ML detection

Ask vendors: "Show me how your system adapts when fraudsters change tactics. Can you demonstrate learning from new fraud patterns in real-time?" Your partner should rely on advanced AI models that continuously learn from millions of unique spending patterns, enabling rapid adaptation to new fraud schemes as they emerge.

Customizable controls

Ask vendors: "Walk me through how you'd customize fraud policies for our specific business model and risk tolerance. What limitations exist?" Every organization faces unique risk profiles and operational requirements. The right partner provides flexible policy management that adapts to your specific needs rather than forcing you into predetermined frameworks.

End-to-end coverage

Ask vendors: "Show me your complete fraud management workflow from transaction monitoring through dispute resolution. How do you ensure compliance at each stage?" Your fraud operations services should include everything from transaction monitoring to dispute tracking, ensuring complete coverage across your fraud management lifecycle.

Transparent results

Ask vendors: "Can you show me exactly how your system makes fraud decisions? What specific metrics will you provide to measure ROI and performance?" Avoid black box solutions. Organizations need to understand how decisions are made and measure the impact of their fraud prevention investments. Expect detailed analytics and reporting that enable continuous optimization.

Regulatory rigor

Ask vendors: "How do you stay current with KYC, AML, OFAC, CIP, PCI, GDPR, and Nacha requirements? Can you show me your compliance update process?" Compliance isn't static—it requires ongoing attention and adaptation as requirements evolve.

Proactive risk management

Ask: "Beyond detecting fraud, how do you help us identify emerging threats and optimize our fraud strategy? Can you share examples of strategic recommendations you've made to similar clients?" Expect customized data analysis and strategic recommendations based on industry-wide trends and your specific risk profile.

Scalability and APIs

Ask: "How quickly can your solution integrate with our existing systems? Can you demonstrate real-time decisioning capabilities and show me your API documentation?" Ensure that they can embed decisioning directly into your existing systems for instant protection and automated dashboards.

Red flags to look for when evaluating fraud partners:

- Inflexible policy management that limits customization
- Lack of concrete performance metrics or unwillingness to share results
- Opaque ("black box") analytics without clear decision criteria that complicates your audit trail
- Lack of real-time detection or decisioning

CHAPTER 3

How to Build a Modern Fraud Prevention Strategy

Effective fraud strategies unite people, data orchestration, and automation across every transaction point. Modern fraud management demands a holistic approach that seamlessly connects technology, analytics, and human expertise to create comprehensive protection, including:

Real-time oversight

Instantly assess transactions—credit, debit, ACH, BNPL, and new payment rails—with AI-driven, dynamic fraud scoring that applies sophisticated risk models to adapt to emerging patterns.

Continuous expert-led risk reviews

Adaptive controls are regularly updated for new threats and compliance changes. Systems should rely on the most recent industry trends and analytic insights for a comprehensive approach.

Automated dispute handling

Streamlined workflows resolve disputes rapidly and surface deeper fraud patterns that might otherwise go unnoticed. Look for solutions that manage the entire dispute lifecycle — aggregating intelligence that adapts with fraud trends.

Customer support

Equip users with tools and resources to recognize, report, and prevent fraud. Education and engagement turn customers into partners in fraud prevention, often catching suspicious activity before it results in losses.

Consortium and network analytics

Broad industry intelligence and network-wide insight enable early detection of synthetic ID fraud, phishing campaigns, romance scams, elder scams targeting vulnerable customers, and emerging threats. This shared intelligence approach allows organizations to benefit from collective learning about new fraud patterns.

Seamless API integration

Advanced APIs embed decisioning directly into systems for instant protection and automated, actionable dashboards. This integration ensures that fraud intelligence reaches every relevant system in real time.

Rising Fraud Risks: Who it Impacts and How to Get Ahead

Fintech companies can't afford to ignore these fraud trends—as AI-enabled scams and account takeovers surge, every compromised customer represents lost revenue, regulatory fines, and brand damage that takes years to rebuild in today's trust-driven financial services market.

KEY RISK CATEGORIES TO TRACK:

Identity fraud

How it Works:
Fraudsters combine stolen and synthetic data (e.g., SSN + fake name) to open new accounts, build ‘clean’ histories, or gain unauthorized access.

Who is Impacted:
Children, immigrants, consumers with limited credit history; anyone whose data is exposed in breaches.

How to Stop Fraud:

- AI identity verification at onboarding
- Cross-institution velocity checks
- Shared fraud consortium data
- Continuous risk scoring

Account takeover

How it Works:
Using stolen or phished credentials, fraudsters gain control of legitimate customer bank, email, or social accounts to steal funds or change personal info.

Who is Impacted:
All demographics, with higher risk for mobile/ online banking users and those with weak authentication.

How to Stop Fraud:

- Behavioral biometrics and device fingerprinting
- Strong, real-time multi-factor authentication
- Login velocity checks and step-up challenges
- fraud engine enabled monitoring

Phishing and impersonation attacks

How it Works:
Criminals send fake emails, texts, or calls posing as trusted brands (banks, agencies, tech support), pressuring targets to click links, enter sensitive info, or transfer funds urgently.

Who is Impacted:
Older adults, new immigrants, less tech-savvy and any digitally active consumer.

How to Stop Fraud:

- AI-driven caller ID/spam call blockers
- Real-time payment/fraud alerts
- Proactive customer education and training
- In-channel fraud scripts and scam warnings

Zelle, Venmo and other P2P payment scams

How it Works:
Scammers request money via a peer-to-peer (P2P) payment app like Zelle, Venmo, or Cash App, often claiming an emergency, posing as bank/tech reps, or faking a transaction.

Who is Impacted:
Banked consumers, especially gig workers, younger adults, and those using P2P payment platforms.

How to Stop Fraud:

- P2P transaction risk scoring and throttling
- Are you sure?' context-based alerts
- Number blacklists and scenario-based transaction blocks

Investment scams (Crypto)

How it Works:
Victims are promised high returns from fake crypto exchanges, Ponzi schemes, or get-rich-quick tips. Scammers may use social engineering or lure through social messaging.

Who is Impacted:
Young adults, retirees, and anyone searching for alternative investments or new tech.

How to Stop Fraud:

- Wallet monitoring and outflow flagging
- Transaction pattern analytics
- Fraud alert overlays for crypto transfers
- Customer education and scam ID tools

First-party fraud —disputes and misrepresentation

How it Works:
Customers make false claims or misuse the dispute process (e.g., claiming a legitimate transaction is fraudulent, overstating losses, misusing chargebacks).

Who is Impacted:
All customer segments; spike often seen in financial distress or rising economic pressure.

How to Stop Fraud:

- Behavioral and transaction analytics
- Dispute pattern recognition via AI
- Education on false claims
- Adaptive thresholds in dispute reviews

Romance and elder scams targeting vulnerable customers.

How it Works:
Scammers build trust over weeks or months (often via dating platforms or social media), then exploit emotionally vulnerable victims for funds or account access.

Who is Impacted:
Singles (especially older women), elders, emotionally vulnerable, isolated or digitally inexperienced users.

How to Stop Fraud:

- AI/ML monitoring of transfer/ communication patterns
- Alerts for recurring risky payment categories
- Digital literacy and scam education
- Adaptive pattern-matching for long-term cons

Business email compromise (BEC)

How it Works:
Fraudsters compromise or impersonate business/vendor emails, requesting urgent wire/ACH payments to fraudulent accounts; also invoice fraud and spear phishing.

Who is Impacted:
Small business owners, company finance teams, anyone authorized for payments.

How to Stop Fraud:

- Payee name verification
- Required callbacks/two-step verification on wire/ACH changes
- Account and behavior monitoring
- Outbound payment analytics

Skimming and shimming

How it Works:
Devices are covertly installed on ATMs, gas pumps, or POS to capture card data from magnetic stripe/chip. Data is cloned and sold or exploited directly.

Who is Impacted:
Debit and prepaid card users at ATMs, POS, or unattended terminals—esp. in high-traffic locations.

How to Stop Fraud:

- Contactless and tokenized payments
- Real-time transaction alerts for suspicious use
- Deactivation of cards used at known compromised terminals

Refund/overpayment scams

How it Works:
The scammer sends 'too much' money (usually via a hacked account) and requests the overage refunded, leaving the victim liable when the original payment bounces.

Who is Impacted:
Small business owners, online sellers (e.g. marketplace users), gig workers.

How to Stop Fraud:

- Hold funds from flagged sources longer
- Automated anomaly detection and AI check validation
- Clear customer warnings against unknown refunds/overpayments

Emerging scams leveraging new technologies

How it Works:
Criminals use new digital tools, AI voice/image/ID spoofing, or exploit new payment rails/platforms as soon as they launch; includes scams not yet seen at scale.

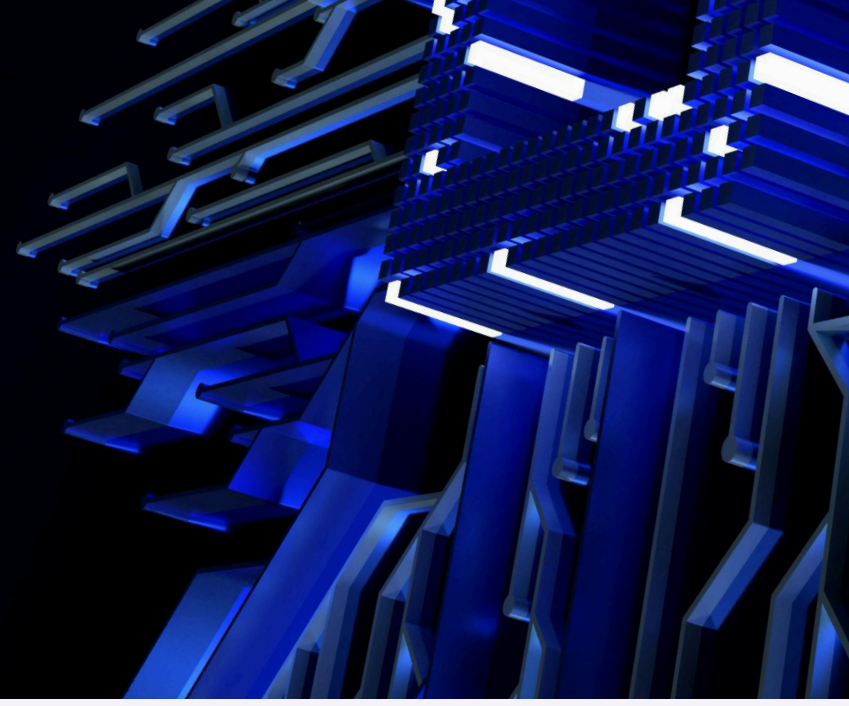
Who is Impacted:
Early adopters, fintech users, anyone exposed to new payments, apps, or unfamiliar communication channels.

How to Stop Fraud:

- Adaptive fraud detection and scenario simulation
- Continuous AI/ML rules updates
- Network/consortium-level early warning
- Real-time education for staff and customers

CHAPTER 4

How Can Financial Services Leaders Enhance Their Fraud Programs?



Banks and fintechs struggling with fragmented fraud vendor portfolios are pushing toward consolidation to reduce complexity and eliminate costly overlaps. A comprehensive fraud program requires a systematic approach that addresses people, processes, and technology simultaneously. Financial services leaders should start with these seven steps:

Assess your risk

Analyze historical fraud trends and vulnerabilities specific to your organization and customer base. Understanding where fraud enters your ecosystem and how it evolves over time provides the foundation for strategic improvements. This assessment becomes even more critical given the consistent upward trend in fraud attacks across all types.

Define your metric

Set KPIs for fraud-to-sales ratio, dispute costs, false positives, and customer experience measures. Clear metrics enable objective evaluation of program effectiveness and guide resource allocation decisions. Having precise measurement capabilities is essential for demonstrating ROI.

Audit resources

You probably already have multiple fraud partners already, but are there overlaps or gaps? Map vendor capabilities, coverage areas, and costs to identify redundancies and blindspots. This reveals consolidation opportunities that reduce complexity while maintaining comprehensive protection.

Layer controls

Use real-time monitoring, post-transaction analytics, automated dashboards, and onboarding intelligence. In-authorization monitoring paired with broader analytics enables comprehensive pattern recognition across all transaction stages.

Choose flexible partners

Prioritize transparency and proven fraud reduction over rigid frameworks or opaque systems. Partners should demonstrate measurable results and provide clear visibility into their decision-making processes. Given the rapidly evolving threat landscape, flexibility and adaptability are paramount.

Monitor and adapt

Regularly review performance and adjust as needed. Fraud tactics evolve constantly, requiring corresponding evolution in defensive strategies. Ongoing fraud services engagement ensures continuous adaptation to new threats.

Educate

Provide alerts, prevention resources, and clear reporting mechanisms for customers. An informed customer base significantly extends your fraud detection capabilities. This education becomes particularly important as AI adoption increases and consumers need to understand how their financial institution is protecting them.

Optimization checklist for fraud program leaders:

- Historical risk analysis and vulnerability assessment
- Clear KPIs for fraud ratios, dispute costs, and customer experience
- Technology audit comparing internal capabilities with partner offerings
- Layered real-time and post-transaction controls
- Ongoing monitoring, adaptation, and customer education

Real-World Results with Galileo

Organizations leveraging the Galileo's Payment Risk Platform (PRP) and fraud operations services have achieved significant, measurable improvements in their fraud management effectiveness.

Case Study 1

A B2C fintech implementing Galileo's real-time PRP controls experienced a 35%+ reduction in fraudulent transactions while maintaining seamless customer experience. The combination of dynamic fraud scoring and customizable controls eliminated false positives that had previously frustrated legitimate customers.

Case Study 2

A digital-first SME banking platform leveraged Galileo's Risk Dashboard and comprehensive fraud analytics to optimize their fraud policies. Through regular consultations with Galileo's fraud operations team and access to the Risk Data Mart, they achieved a 15% improvement in fraud detection accuracy while reducing false positives. The performance insights enabled data-driven policy refinements that enhanced both security and customer experience.

Case Study 3

Clients using Galileo’s Card Transaction Risk Gscore (Gscore) - a machine-learning-based risk score that assesses the risk of card transactions in real time - on average saw fraud loss savings of 18% and fraud dispute OPEX savings of 11%. In addition they saw additional improved transaction volume of 24 basis points (bps) which improved revenue interchange 8bps on average.

Case Study 4

A leading online banking service implemented Galileo's PRP Risk Dashboard and consultation services to continuously refine their fraud strategy. Regular performance reviews and access to aggregated trend analyses enabled them to stay ahead of emerging fraud patterns, resulting in improved policy effectiveness and enhanced customer trust through proactive fraud prevention.

These results demonstrate that effective fraud management isn't just about preventing losses—it's about enabling business growth through enhanced customer trust and operational efficiency.

The Galileo Payment Risk Platform: A comprehensive approach

Nothing damages customer relationships faster than blocking legitimate transactions or creating unnecessary friction during critical moments. That's where Galileo's Payment Risk Platform , an AI-powered fraud detection and risk management platform, provides real-time risk intelligence that distinguishes between genuine threats and normal customer behavior, ensuring security without compromising user experience.

Users can achieve the best response for each customer by combining real-time controls (in-authorization monitoring) with thorough post-transaction reviews and channel-wide monitoring. This dual approach catches threats at multiple stages—preventing losses during the transaction itself while learning from patterns that emerge over time. The Galileo Instant Verification Engine (GIVE), enhances this capability by providing immediate identity verification of external bank accounts to confirm their existence, status, and associated risk signals during critical moments.

The most effective fraud programs recognize that customization requires more than tweaking existing rules, it also integrates with business operations. Organizations using Galileo's Fraud Operations benefit from continuous risk consultation that adapt their strategy as threats emerge and business needs evolve. In the first half of 2025, the Galileo Fraud Operations team saved clients over $1.2M in the areas of identity, first-party, ACH, dispute abuse and elder abuse fraud.

ADAPTABLE STRATEGIES THAT HELP ORGANIZATIONS MOVE FASTER AND PROTECT THE CUSTOMER EXPERIENCE

Dynamic fraud programs, supported by analytics, adaptable technology, and expert consultation, can transform fraud prevention into a business asset. For financial institutions, fintechs, and brands, a proactive approach reduces risk and cost while driving customer trust, efficiency, and growth.

Proactive fraud management delivers:

- Reduced risk and operational costs
- Enhanced customer trust and satisfaction
- Competitive advantage through superior security
- Foundation for sustainable business growth

Why Clients Choose Galileo for Fraud Services

Galileo delivers scalable, efficient operations that align with regulatory standards and evolving fraud trends. Our deep expertise in fraud detection and risk management lets clients focus on core business growth while protecting their customers.

End-to-end fraud coverage

From real-time detection to case investigation and resolution, Galileo provides comprehensive fraud services tailored to each program's unique needs.

Regulatory compliance

Our team enables adherence to KYC, AML, OFAC, and Nacha guidelines, minimizing compliance risk.

Customizable solutions

We design fraud controls that fit specific risk profiles, program goals, and customer experience expectations.

Advanced technology

Leveraging industry-leading tools, data analytics, and machine learning, we stay ahead of fraud trends while minimizing false positives and operational friction.

Operational excellence

Our dedicated fraud teams follow detailed investigation protocols, root cause analysis, and clear documentation practices—ensuring quality case handling and SLA adherence.

Proactive risk management

Beyond detecting and servicing fraud, we identify emerging threats, recommend rule adjustments, and share insights to enhance clients' overall fraud posture.

The evolution from reactive fraud management to proactive, customer-centric strategy represents more than just operational improvement. It creates competitive advantage. Organizations that embrace this transformation position themselves not just to survive the current threat landscape, but to thrive despite its challenges.

The key lies in understanding that modern fraud management is fundamentally about balancing:

- Security with customer experience
- Real-time protection with post-transaction analysis
- Automated intelligence with human expertise.

By integrating multiple fraud prevention tools—including risk platforms, verification systems, and operational consulting—organizations can shift fraud management from purely defensive spending to strategic business value.

galileo

Are you ready to boost your payments fraud detection — and protect your customer experience?

Galileo provides a comprehensive approach to fraud detection, while reducing risk and improving ROI.

Fraud prevention that works for you

Whether you're tackling fraud in credit cards, ACH, BNPL, or instant payments, Galileo provides the tools you need to detect, prevent, and mitigate financial crime before it impacts your bottom line.

Experienced fraud analysts by your side

Throughout the Galileo fraud services engagement with our clients, we provide a continuous risk consultation, using the most recent key trends from the industry, our consortium data and analytic insights for a comprehensive approach to combat fraud.

Ready to engage with a fraud specialist?
Contact us today for an assessment of your fraud

galileo-ft.com Contact Us