The Anti-Fraud Playbook

Your Guide to Lowering Fraud Losses and Minimizing Payment Risks in 2023

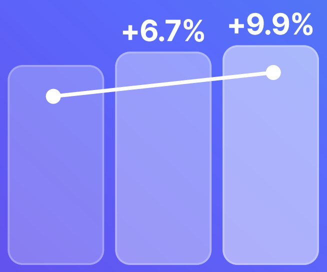
galileo

Modern Fraud Requires Modern Fraud Mitigation Solutions

Today's fraudsters aren't just stealing credit card numbers—they're using smarter, more sophisticated methods like faster-than-fingers bots to swiftly commit complex payments fraud schemes that are getting increasingly harder to detect in a timely manner. The fallout is costing businesses nearly $30 billion a year.

Fraudsters are using advanced tools that make it more complicated and harder for financial institutions (FIs) and non-FIs to keep pace. With instant access to banking, transfer and payment options across multiple channels and devices, fraudsters have more opportunities in more places than ever before.

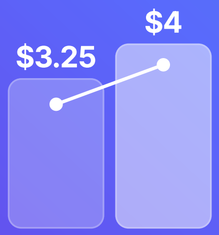
Newly discovered vulnerabilities are compromised sooner and more frequently, and the costs add up quickly.

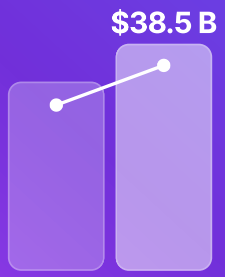


The Rising Cost of Fraud for Financial Services has increased between 6.7% and 9.9% higher than pre-pandemic years.

Cost of fraud = time, money, productivity, reputation and customer relationship costs incurred by financial services providers in dealing with the fallout of fraud incidents.

When $1 is lost to fraud, the FI loses as much as $4 —a number that has risen from $3.25 per $1 in 2019.





Payment card fraud transactions are forecast to rise 20% to $38.5 billion by 2027, as fraudsters continue to employ more sophisticated techniques.

Mitigating fraud in-house alone is also becoming increasingly more difficult as banks, fintechs and program managers often lack automated systems, access to trend data and comprehensive processes that allow them to maintain and demonstrate compliance—especially at scale. Organizations are quickly learning that a manual approach won't cut it–and smart firms are deploying sophisticated AI and machine learning-based tools that provide actionable data.

But knowing how to establish a robust anti-fraud framework requires a deeper understanding of multi-layered authentication processes, dynamic fraud decisioning and real-time insights. While you're busy growing your business and concentrating on the customer experience, you shouldn't have to worry about how to mitigate fraud. That's why we've created this playbook:to provide an insider's look into the risks spreading across today's payment fraud ecosystem and arm you with actionable steps to get ahead of the fraud risks that likely already exist across your organization.

Read on to sort through the noise and learn what to look for in a payments fraud management partner as you look to lower your fraud losses and minimize payment risks.

Inside the Anti-Fraud Playbook:

Ditching the Reactive Approach:

The Power of Tech, Data and People

Even as technology has advanced, many organizations still rely on outdated, manual review processes that spot payment fraud only after it has already occurred. This reactive, costly approach leaves businesses playing catch-up–and clean-up, repairing customer relationships and taking on an unnecessary level of fraud losses.

These manual and time-intensive approaches simply don't cut it for today's fraud environment, as bad actors rush to stay one step ahead and move on to the next fraud scheme long before being caught.

Instead, a modern fraud mitigation strategy involves a scalable approach that replaces manual, labor-intensive interactions with AI and machine learning tools that use hundreds of millions of data points to identify and analyze patterns and identify anomalies that may pose impending threats before they escalate. This proactive approach anticipates risk and leverages multi-layered authentication processes and fast fraud decisioning to stop fraud before it takes place.

Relying on a tech-centric solution that taps into the power of AI and machine learning doesn't mean ditching human instincts all together, so don't overlook the value of human expertise when evaluating a payments fraud protection partner.

The best fraud mitigation solutions are built by fraud industry experts who have spent decades learning how fraud risks have evolved, and have a documented and tested approach to applying those insights–and the know-how to use technology to create fraud mitigation models that continually get smarter over time.

For Galileo, it's not just the modern technology that counts; it's the people, combined with the data analytics and technology, that creates the holistic approach.

No matter how much fraud data an organization has, or how sophisticated their payments or eCommerce fraud detection technology is, it's the people behind the technology that make the insights gathered from payments data actionable through a comprehensive fraud management program.

Where to start?

Benchmarking Your Fraud Appetite: Actionable Tips to Make Your Fraud Mitigation Strategy Count

It's commonly understood that fraud losses are part of the cost of doing business. Perhaps, but how much fraud is too much? Every company wants to minimize fraud, but at what cost?

What is an acceptable amount of fraud for your card program? Are your fraud benchmarks off? Are you "accepting" too much fraud across your organization for fear of turning away a good customer? This is a delicate balance that all teams must consider.

Unfortunately, there's no simple equation here, as payment fraud volume varies depending on the size of your organization, the volume of transactions you're processing, what channels you're operating on, and what type of industry you're in.

Establishing meaningful fraud benchmarks for your business requires numerous considerations, including your company's risk appetite, the financial products you offer, and more. The quickest way to understand how to solve that equation is with a trusted fraud mitigation expert that has full visibility into where fraud is occurring, how much is occurring, and how much of that is preventable. From there, you can establish benchmarks for your organization to work toward.

Of course, when it comes to fraud, zero is always the goal, but never the reality. Still, there are fraud management KPIs—such as dispute rate or fraud rate/loss per client— that you can measure how effective you are at reducing specific types of fraud. When considering what fraud types to watch for, four key types of fraud we are often tracking include:

Four Fraud Categories to Watch:

- First-Party Fraud
- Account Takeover Fraud
- eCommerce Fraud
- Synthetic ID Fraud

1. First-Party Fraud

60% of financial institutions report that first-party fraud is their top concern and the cause of most lost dollars. First party fraud involves an abuse of an individual's account by the account owner with an intention to take advantage of its monetary value. This is commonly accomplished by applying for a loan or credit card they won't pay back, or misrepresenting their financial situation to get a more favorable rate.

First-party fraud is characterized as either opportunistic—perpetrated on a small scale by a single fraudster or an informal group—or organized, carried out at scale by a criminal gang or ring.

The biggest challenge with first-party fraud is that real individuals often commit these crimes, and they can pass through many mitigation filters thanks to having established, known identities. It takes a sophisticated machine learning solution that has the power to identify suspicious behaviors based on IP address, time between transactions, and other behind-the-scenes data to identify this type of fraudulent activity.

2. Account Takeover Fraud

Account takeover fraud is one of the most common identity theft schemes today, and involves fraudsters gaining access to someone's financial account. During the 2021 holiday shopping season, 1 in every 140 login attempts was an account takeover.

This type of fraud is very hard to detect and prevent because it occurs over a series of small steps that often occur under the fraud radar of many organizations. This is why more than half of individual victims were unaware of a breach until they logged in and noticed unfamiliar activity or missing funds.

The key to catching account takeovers is having access to massive amounts of aggregated transaction data that recognizes authentic account patterns and reveals behavioral anomalies. When fraudsters use stolen PII, or personally identifiable information, they often don't behave like typical buyers. Sometimes, fraudsters start with a small test transaction before making a big purchase; other times, they open multiple accounts in the victim's name to enable even more fraud.

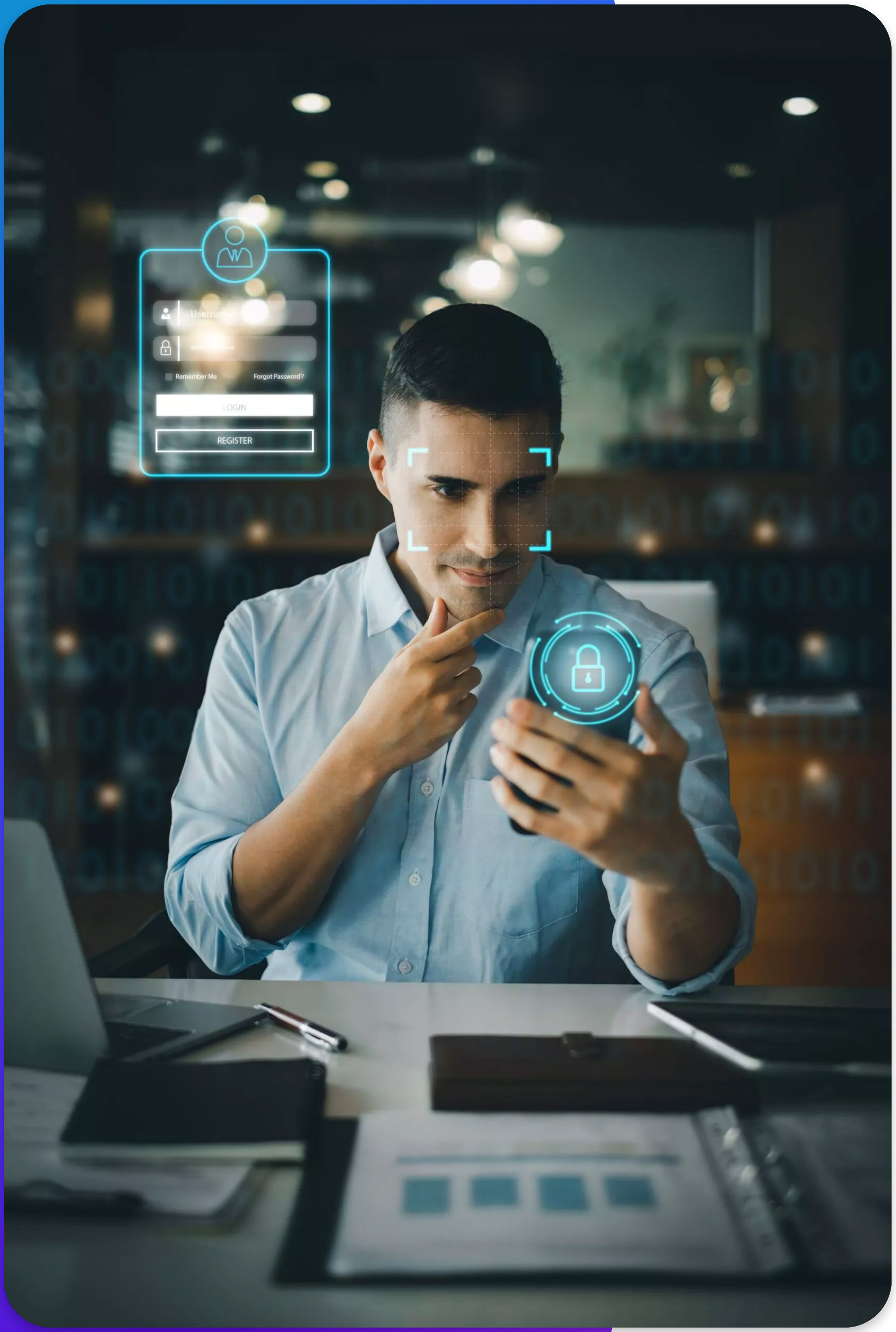
It's particularly difficult to proactively identify account takeover fraud using manual methods because it appears the transaction activity is being committed by a legitimate person. By the time the fraud has occurred, it is often too late to stop the damage — leaving the FI or business to cover the cost and manage a damaged customer relationship. Javelin reported that account takeover losses increased 90% in 2021, which is why automated machine learning that detects suspicious account behavior before the fraud has been committed is so critical to spotting these bad actors in real time.

Having access to various types of consortium data, allowing proper client authentication mechanism at login and developing automated knowledge graph capabilities to identify various linkages of spend will help mitigate these issues, even when it can't solve 100% of each problem.

3. eCommerce Fraud

ECommerce fraud continues to rise; it's projected to cost $40.62 billion in 2027, yet only 34% of companies invest in detecting and preventing it. It's a big problem for both B2C and B2B businesses and requires companies to continually stay up to date on top eCommerce fraud trends as more and more transactions shift online.

Manual, human-run fraud mitigation processes fail to provide full visibility into risky transactions at the speed needed to keep up with today's fraudsters. But powerful algorithms that rely on millions of data points can. Similarly, no person could filter through those millions of transactional details required to surface fraudulent patterns. Today's eCommerce fraud patterns require rapid response and intelligent decisioning derived from artificial intelligence (AI) and machine learning models.



4. Synthetic ID Fraud

The challenge with synthetic ID fraud is that there's no consensus on how big of a problem it actually is. Industry estimates peg the cost of synthetic ID fraud at anywhere between $6 billion and $20 billion as this type of fraud is incredibly hard to spot and often goes unreported.

Synthetic ID fraud is when fraudsters create fake identities, slowly layering on "real-looking" details using potentially valid social security numbers with accompanying false personally identifiable information (PII). This can even include other personal details such as phone numbers and social media accounts. At some point, the "identity" starts applying for loans or lines of credit, and by the time the FI catches on, the horse is already out of the gate and the fraud has been committed under an identity that doesn't actually exist.

Synthetic ID fraudsters are increasingly problematic for FIs because they can generate an unlimited chain of accounts, making them hard to root out. Fortunately, today's fraud prevention providers can use machine learning models to show in real time what behavior is occurring, where it is occurring, and spot anomalies that indicate suspicious activity. That can trigger fraud mitigation tools to flag the activity for further evaluation and stop the potential fraud in its tracks.

Making Your Fraud Mitigation Strategy Count:

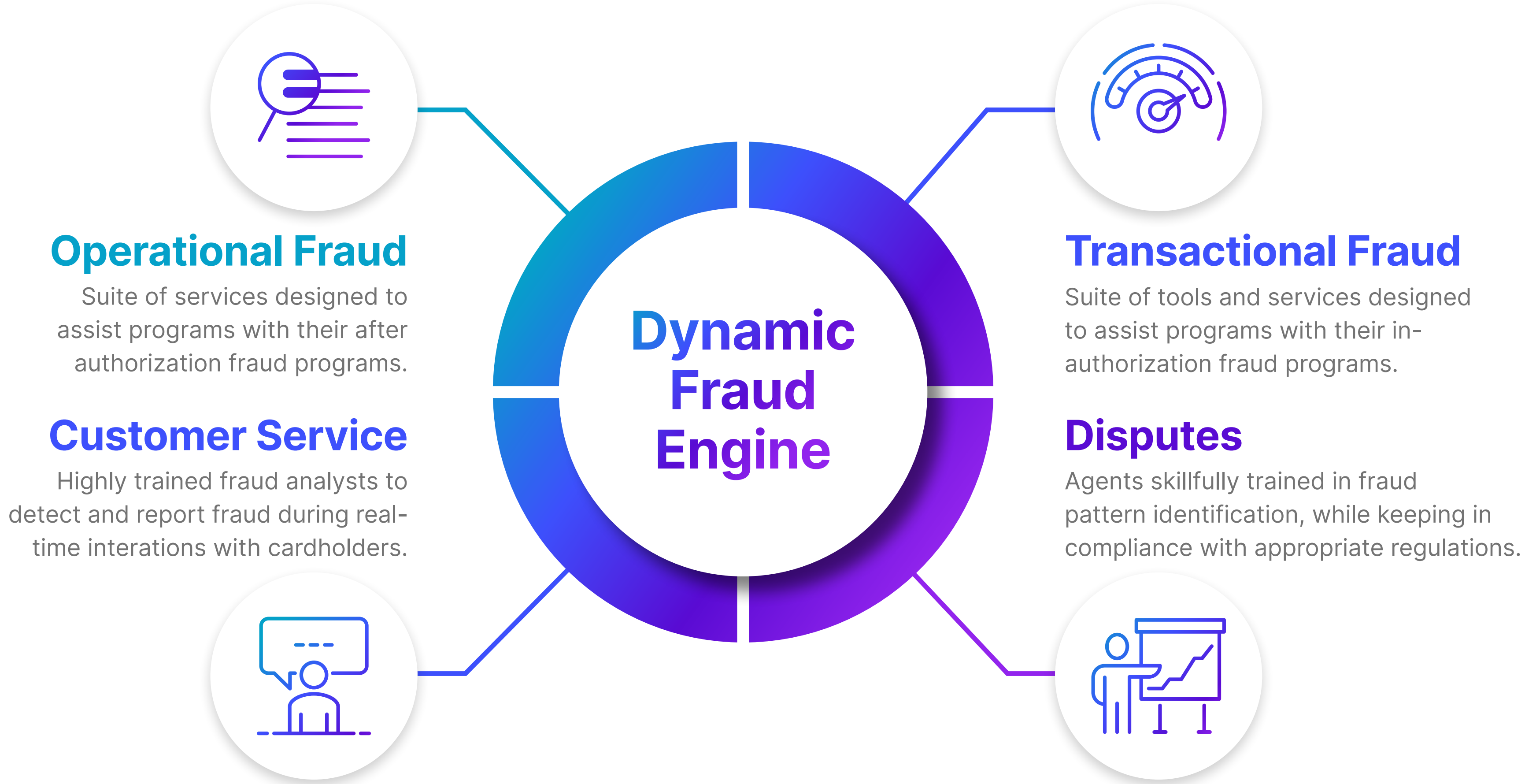
Six Tips to Consider

Modern fraud prevention requires spotting risk early, consistently and quickly. You must rely on a multi-layered approach to proactively lower fraud losses and minimize payment risks.

> **“Effective fraud solutions must ‘listen’ to multiple data elements simultaneously. By running models on top of the company’s data, the AI can identify emerging fraud trends. Real-time data needs to flow smoothly, and legacy platforms can create information bottlenecks.”**
>
> ***– Maxim Spivakovsky,*** *Senior Director of Global Payments Risk Management, Galileo Financial Technologies*

Tip 1: Target fraud at every point in the transaction—adopt a holistic approach

Addressing payments fraud throughout the entire transaction maximizes opportunities to identify and stop fraud and consists of four key elements:



Dynamic Fraud Engine

Operational Fraud

Suite of services designed to assist programs with their after authorization fraud programs.

Customer Service

Highly trained fraud analysts to detect and report fraud during real-time interations with cardholders.

Transactional Fraud

Suite of tools and services designed to assist programs with their in-authorization fraud programs.

Disputes

Agents skillfully trained in fraud pattern identification, while keeping in compliance with appropriate regulations.

When offered together, transactional and operational fraud mitigation, customer service, and dispute resolution are the pillars of today's most powerful solutions.

A modern, holistic fraud mitigation solution is fast and responsive.

The most essential parts of any well-built fraud mitigation machine include:

- Detailed, customizable program parameters
- Extensive compliance measures
- Adjustable risk controls
- Ongoing, real-time network checks
- A real-time fraud engine with multi-layered controls and mitigation strategies

Characteristics of Holistic Fraud Solutions

Network Checks

Sanctioned Merchants

Proprietary Fraud Engine

(Rules and Machine Learning Models – in-house & 3rd Party)

Program Parameters

e.g. No ATM transactions allowed

Compliance Measures

e.g. Transaction requests from sanctioned countries

Risk Control

e.g. Invalid pin, AVS check

Tip 2: Familiarize yourself with the advantages of machine learning

The advantages of machine learning-based fraud mitigation solutions are vast. Machine learning:

- Uses computer algorithms to analyze billions of data points to identify fraud patterns
- Learns specific industries and niche markets over time
- Can simultaneously run multi-layered detection algorithms
- Provides near-instant onboarding for new customers
- Is easy to scale as business grows

Tip 3: Address Fraud at the Right Speed: Green, Yellow and Red Rules Get Smarter Over Time

To help clients calibrate their fraud management and risk tolerance, Galileo has created a green, yellow and red analogy that corresponds to Go, Add Friction and Freeze. This also translates to authorize, slow down or stop. This strategy allows organizations to effectively target fraud risks at the appropriate urgency level. Over time, the application of this stoplight strategy ensures transaction behavior is continually evaluated at the proper risk level, and in the right time frame.

For instance, for known fraud, the freeze allows for the action to be stopped immediately to block the attempt of the bad actor before the risk spreads. Galileo also enables what we call the “friction for authentication approach,” which involves blocking fraud attempts, while simultaneously requesting a client reach out for identity verification and authentication.”

The yellow—or the add friction—approach allows for real-time analysis of the potential fraud to determine what action to take next. The green—or go—also allows for this analysis to be completed so good customers aren’t unnecessarily stopped from completing a transaction.

The goal of this approach is to classify each transaction into a category (green, yellow or red) that provides better visibility so a risk decision can be made. Performing these proactive identifications before a transaction has been fully processed arms organizations with actionable insights into what is occurring across their card portfolio in real time so they can identify threats before they come to fruition.

This method gets fine-tuned as more data (i.e., more transactions) are added to a client’s portfolio and more sophisticated fraud and risk recommendations can be made over time. By providing better visibility into potential fraud patterns, businesses can make more proactive decisions that align risk levels with the right mitigation path.

Tip 4: Take a Multi-Layered Approach to Fraud Mitigation

To pinpoint operational and transactional fraud risks organizations need access to fraud intelligence delivered from millions of unique spend patterns. This can be achieved through fraud mitigation tools that have the following:

- **Data layer:** An ability to analyze all the info that's coming from your transactions that can help you navigate from one fraud mitigation layer to the next.
- **Detection/Transaction layer:** As patterns emerge from transactions, there are signals within the detection layer that indicate if and when there are risks.
- **Fraud operations layer:** An ability to catch or identify fraud that's happening or about to happen. It's important to identify vulnerabilities outside the payment process itself, including payment disputes, to determine when true fraud is occurring or about to occur.

Tip 5: Avoid the 'Set-it-and-Forget it' Approach. Balance Unsupervised Vs. Supervised Machine Learning

As tempting as it is to "set it and forget it," that's not how a modern fraud solution works best. The value of machine learning models is that they can continually adapt to patterns, but you must have trained fraud experts to make sense of all that data to tailor effective risk controls.

This holistic view of financial activity requires a higher level of interaction with sophisticated data models that most organizations simply don't have the time, resources and expertise to manage. That's where Galileo fits into your fraud reduction strategy.

The difference between machine learning models:

- **Unsupervised models:** Generating a model based upon historical data, this approach plugs data into the system and does not require any additional interaction or learning to work. While this model can sustain itself, there are limitations since there is little oversight to ensure the models are catching the right types of fraud at the right time.
- **Supervised models:** Require human interaction to validate activity. While this requires more time to ensure the machine learning models are working, the combination of people, data and technology makes this approach more impactful because of the ability to spot potential fraudulent activity faster, and take actionable steps to stop the spread of the potential fraud risks.

At Galileo, we advocate a hybrid model that allows for unsupervised and supervised models to work in tandem to ensure there are no gaps in your fraud mitigation efforts.

Tip 6: Use Data to Understand Common Points of Compromise and Proactively Protect Against Them

Without the expertise of a third-party fraud solution, most companies lack visibility into common points of compromise, such as card skimmers, and common test locations for fraudsters,such as gas stations or ATMs.

A holistic solutions provider like Galileo will use data from across the ecosystem and deploy risk models on your behalf that identify and alert you to likely points of compromise so you can block or otherwise address the potential threat. This leads to less fraud and improved customer satisfaction.

This proactive approach allows Galileo to identify the compromised locations, the cards associated with that compromise, and the ability to extend clients the opportunity to act on multiple fronts. Those actions include replacing the card for the cardholder, providing expensive monitoring of these cards, or alerting the cardholder about the potential fraudulent activity on the horizon. We also provide guidance on how to avoid the issue in the future.

Five Things to Look for in a Fraud Mitigation Partner

Now that you have an understanding of some of the greatest fraud threats that exist across the payments ecosystem, it's time to look at the key considerations to take into account when choosing a fraud mitigation partner.

Primary Types of Payments Fraud

1. **Transactional fraud:** fraud that occurs during the transaction, including:
   a. Compromised card fraud
   b. Merchant fraud
   c. Session replays
   d. Fraud due to Account Takeover
2. **Operational fraud:** fraud that occurs after the transaction, such as:
   a. Fraudulent returns
   b. Friendly fraud (chargebacks)
   c. Lost or stolen merchandise

Organizations must:

1. **Look for customized solutions that can support your company's transaction and risk profile.** There are many nuances in the payment risk and fraud ecosystem. A partner must provide an agile suite of proactive fraud mitigation services to target evolving fraud risks that apply to your product and program profiles.
2. **Look for multi-layered solutions that offer comprehensive fraud and risk protection.** For a future-proof fraud solution, it's important to rely on technologies that can actually get "smarter" as they ingest more data over time.
3. **Expect better risk decisioning with actionable, real-time data for card-based transactions.** Many forms of fraud involve cards. Experience proactively identifying, flagging and declining potentially fraudulent card transactions in real time with AI and dynamic data analysis helps avoid other after-the-fact processes, such as chargebacks.
4. **Demand a holistic, tailored strategy that handles end-to-end payments fraud services.** A truly modern fraud and risk platform addresses both operational and transactional fraud, unlike legacy systems that focus solely on transactional risks.
5. **Save time, money and headaches by outsourcing customer service and disputes.** A fraud mitigation partner should also provide top-notch customer service, including digital tools and a team of people who can step in when only a human will do: for resolving false positives, helping customers, and settling disputes.

"I spend my day reviewing our client's data and performing detailed analysis of transactional fraud. My team focuses on remediating and preventing emerging fraud trends, which allows Galileo the ability to dynamically interrupt a fraud event in real time. Fraud can have a significant impact on operational costs and client experiences. This is why our Galileo Dynamic Fraud Engine product is a critical piece of the puzzle in mitigating fraud."

– Shelley VanZomeren, Senior Transaction Analyst at Galileo

Why Galileo?

Get smarter about fraud with access to datasets—and experts who make that data actionable for your team

Through an array of algorithms, Galileo's solution targets every corner of the payments ecosystem by combining fraud analytics and advanced machine learning technology to create a uniquely powerful platform.

Galileo provides a real-time transaction risk assessment, near-real time fraud risk analytics and strategy assessment of rules, merchants, location activity, etc. Galileo also provides ongoing fraud monitoring systems and risk model performance assessments for offline monitoring.

Data

Galileo uses data-driven insights to drive smarter decisions that improve the customer experience while keeping fraud out.

Scalability

As your business ecosystem grows, the impact of your technology and data investments grows with it. Galileo's team of fraud experts are equipped to advise clients on the right solution/card program based on their transaction volumes to target their greatest fraud risks.

ROI

Reducing fraud risk and improving ROI can, and should, be done together. On average, Galileo clients achieve a 35% reduction in fraud transactions, and that's because we help our clients proactively get ahead of fraud risks with access to more than 100M unique spend patterns.

A forward-thinking approach to fraud mitigation

Our access and connections to the payments ecosystem enables Galileo to tailor our clients' risk strategy and recommendations.

Galileo Provides:

- **Enhanced fraud monitoring capabilities** with near real-time fraud risk analytics and strategy assessment of rules, merchants, location activity, etc.
- **Ongoing/additional fraud monitoring systems** and risk model performance assessments for offline monitoring.
- **Highly trained fraud analysts** who help clients with fraud and dispute strategies (with proper compliance protocols), and a customer service team who works with clients and cardholders when fraud is detected.
- **Continuous risk consultation**, using the most recent key trends from the industry, consortium data and analytic insights for a comprehensive approach to combat fraud.
- **Real-time decisioning** using network risk checks, program and account level controls, advanced rules enhanced by machine learning-based models, and a rich data store.
- **Speed to Launch:** Galileo can help partners take action in as little as a few weeks.
- **Our open APIs** make it easy to add Galileo's fraud protection to a company's existing technology stack, and we're here to help every step of the way.

Take the next step with Galileo

Let Galileo help your company mitigate payments fraud risk with our proven, purpose-built technology. Galileo helps you offload operational complexities and save time, money and resources. Most importantly, we can help you save your customers from the frustration and inconvenience that false positives and payments fraud can cause.

Ready to engage with a trusted fraud specialist? Reach out today for an assessment of your fraud management strategy and learn how we can help you lower your fraud losses and minimize your payment risks. **Contact us to start a conversation today.**

galileo