paladin vendor report | **fraud prevention**

2026

TENTH ANNIVERSARY

paladinfraud

Thank you for downloading the Paladin Vendor Report.

The Merchant Risk Council's (MRC) mission is to provide members with useful tools and sometimes scarce information to help lower fraud and improve your customer's purchasing experience. At the MRC, we understand how difficult it is to navigate a complex ecommerce environment and find the right solution for specific fraud and risk needs. As a benefit of your MRC membership, we are offering members a discounted copy of the Paladin Vendor Report (PVR).

The PVR, gathered by the industry experts at Paladin, provides detailed information on over 50 vendors who offer a wide variety of different fraud prevention tools, platforms, and services. This report is designed to give you a comprehensive overview of the different products offered by each company and present analysis to help you focus on who may ultimately best align with your individual fraud prevention goals.

We hope you find this report to be a helpful resource that will provide you and your business with valuable insights. We are also interested in hearing your feedback on the report and encourage you to send any comments directly to programs@merchantriskcouncil.org.

Sincerely,

The MRC

Table of Contents

The 2026 Paladin Vendor Report

The commerce landscape is increasingly complex. This report cuts to the chase. Every day at Paladin Group, we're in the thick of the fast-paced world of fraud solutions. With dramatic changes coming quickly, including AI "assistants" or "Agents" handling shopping tasks on the customers behalf, commerce and business models are ever-evolving. So it's crucial to remain focused on streamlining and maximizing the capabilities of organizational fraud management operations while reducing checkout friction and preparing technology to identify legitimate agent-led activity without increasing false positives.

As experts on today's solution providers, services, and tools, it's our job to maintain a high-level view of the fraud prevention landscape as well as a detailed, on-the-ground understanding of every solution and every challenge. As the number of providers and services grow and technology evolves, merchants' options become increasingly complex and varied.

It's our mission to serve as an authority on these products and their strengths, areas of opportunity, and enhancements, which is why we published the first-ever Paladin Vendor Report (PVR) in 2017. It offered an unprecedented exploration of how merchants could mitigate the risks that come with accepting payments in an omni-channel, card-not-present world.

Because of the constant evolution of many popular fraud mitigation solutions, we decided to provide the Paladin Vendor Report (PVR) on an annual basis. And now, we're pleased to publish the latest: the 2025 Paladin Vendor Report. We've offered

We focus on several key areas during the discovery process. (Not all are applicable to every vendor, but for consistency, we examined each of the following wherever relevant.)

PRODUCT - The vendors overarching solution and functionality.
SERVICES - Available offerings to help merchants during integration and throughout their client lifecycle, including reporting.
BUSINESS DEVELOPMENT - Current partnerships and channels for direct and indirect customers.
MARKETING - Industries and verticals of focus.
SALES - A breakdown of marketing and sales.
TECHNOLOGY - Integration and technical details associated with the solution.

previous participants the chance to update their sections and incorporated additional participating vendors.

What this report offers: the PVR helps merchants navigate the ever-expanding number of solution providers and services available to them. We spoke with vendors who offer risk mitigation products to merchants in the Card Not Present (CNP), omni-channel, marketplace, and fintech environments—then gathered, examined, and compiled the information for each participating vendor.

Vendors had the option to participate in the report, and Paladin was compensated for the research performed. Our team spent hours in discussion with each of these vendors. We test-drove their products and gathered overviews of their services, marketing, sales, technologies, and future plans. For vendors who chose not to participate in the report, we drew upon our extensive interaction, client input, and research to share a summary of their services.

This report is a groundbreaking effort to gain as much first-hand knowledge as possible from fraud prevention vendors, compiling our findings in a way that's helpful and revolutionary for our industry and the merchants who depend on us. This report is purely informational, and it is not designed to rate the products and services of the vendors, review them, give opinions on them, or give a thumbs-up (or down) about the vendors. The report's intent is to provide clarity regarding what products and services fraud mitigation vendors offer.

The vendors are segmented into five different categories based on their core offerings. Some of the vendors offer other products that complement their core offering or have additional functionality or products. Some vendors provide services in overlapping segments, and this report offers a separate overview for each of the following categories:

- User Behavior & Reputation
- 3DS & Consumer Authentication
- Fraud Platforms & Decision Engines
- Identity & Data Verification
- Chargeback Management & Platform

Core functionality icon key

3rd Party API Capabilities – The ability to call out via API to third-party vendors for data, device fingerprinting, etc.

Payment Gateway Capabilities – The ability to process payments directly through their own platform or solution.

Operational Support – Provides outsourced operational support, at a cost, for reviewing high-risk transactions and/or managing chargebacks.

AI Powered – Matching algorithms to detect anomalies in the behavior of transactions or users.

Guaranteed Chargeback Liability – Guarantees merchants do not take fraud losses for vendor-approved transactions.

ATO Detection Capabilities – Using device characteristics to detect account takeover/ account penetration.

Account/Client Management – Personnel dedicated to working directly with clients.

Device Fingerprint Capabilities – Built directly into the platform (not a third-party API call).

Historical Sandbox Testing – Ability to test rules against historical transactions in a non-production environment.

Professional Guidance/Services – Provides outsourced support for data analysis, rules-building, and recommended best practices, etc.

User Behavior Capabilities – Built-in (not via third-party) capabilities to capture cursor movements, mouse clicks, and time on a merchant site.

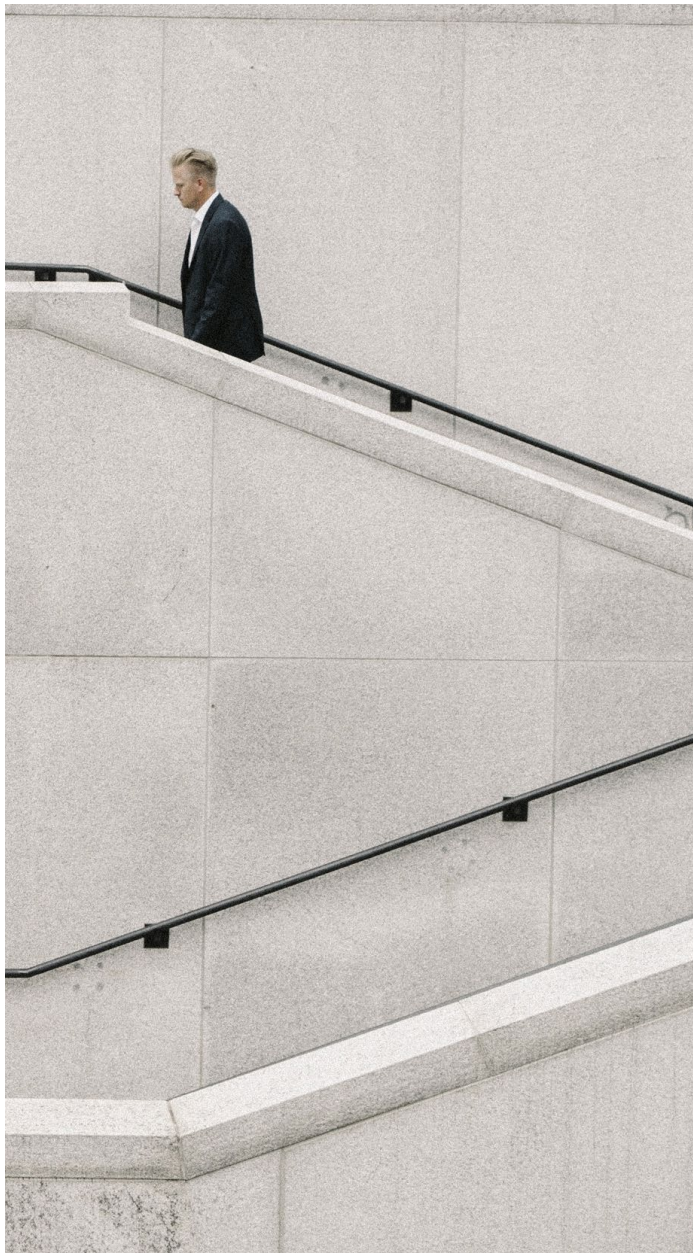
Pre-Authorization Functionality – Ability to score and/or decision a transaction prior to authorization.

Fraud Engine/Platform Functionality – Ability to score/decision a transaction post-authorization.

Non-Production Real Time Rules Testing – Ability to test real-time transactions in a non-production environment.

User Behavior & Behavioral Biometrics

These solution providers offer logic designed to track users and prevent malicious activity by capturing and analyzing behavioral characteristics across the entire session, from login to check out and everything in between. These solutions compare known customer behavior in the case of an existing account. They also assess whether behavior is low or high risk relative to the overall order volume. Merchants and financial service providers can use these additional data points as an added layer in their greater process, or make a decision on them directly.



BioCatch

When it comes to fraud prevention and anti-money laundering, **BioCatch** believes that customers are an important part of the solution. They believe getting to know them, their idiosyncrasies, their digital habits – the when, how, where, and why they bank and check out – is all part of their unique journey and relationship with a brand. Customers do not have to be the weak link in a fraud prevention and anti-money laundering strategy.

In partnership with their 100+ customers, **BioCatch** has proven that if you pay close attention to the behavior and intent behind the biometrics, device, geo-location, and other machine-created signals, they can empower you to deliver your customers a seamless digital banking experience free from fraud and safe from criminals.

And for fraud, AML, and cyber security teams, they can deliver meaningful reduction in fraud, ease the burden on operations teams, and proactively identify bad actors and accounts while connecting organizations to the most curious, experienced, and thoughtful community of Fraud Fighters on the planet.

BioCatch

At a Glance:

ATO Detection Capabilities

Account/Client Management

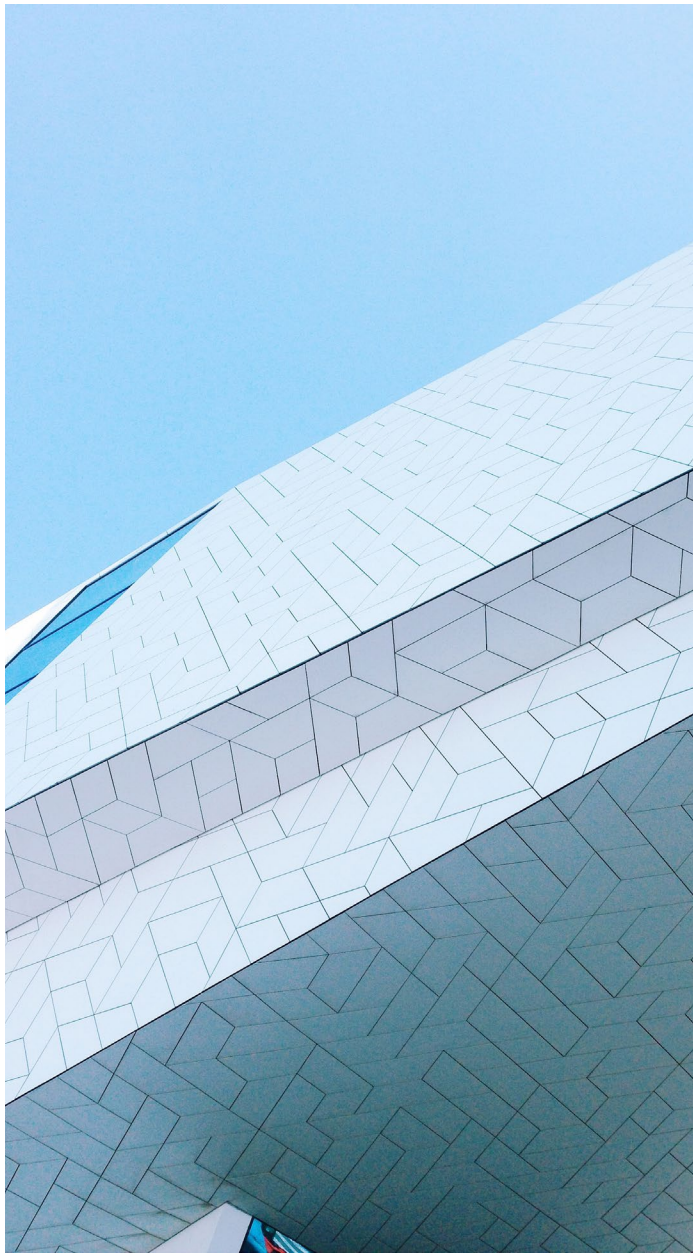
Pre-Authorization Functionality

BioCatch chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

3DS & Consumer Authentication

3DS refers to a protocol designed to add an additional security layer for online credit and debit card transactions. The additional security layer helps prevent unauthorized Card Not Present (CNP) transactions and protects the merchant from CNP exposure to fraud. Each of the card brands have their own product designed specifically for the protocols: Visa has Verified by Visa, Mastercard has Mastercard SecureCode, American Express has American Express SafeKey, and Discover has ProtectBuy. There are companies providing products and services encompassing all four card-branded products.

A new variant, 3D Secure 2 (3DS2), is designed to improve upon 3DS1 by addressing the old protocol's pain points, and it delivers a much smoother and integrated user experience.



Accertify 3D-Secure

Accertify understands that customer expectations are ever evolving and so is fraud. Today's online consumers expect to be recognized and rewarded as loyal customers. They want to transact with a single click from any device and feel confident their account is secure. At the same time, each online event exposes your organization to reputational and financial risks that can have a material impact.

Trusted by many of the largest companies globally, **Accertify** is a leading digital platform assessing risk across the entire customer journey, from account monitoring and payment risk to refund fraud and dispute management. Accertify built a comprehensive platform with integrated solutions across the entire customer journey, letting organizations see the complete picture and proceed with confidence. **Accertify** can help reduce the need to juggle multiple vendors and decipher fragmented risk scores that result in unwelcome friction for customers.

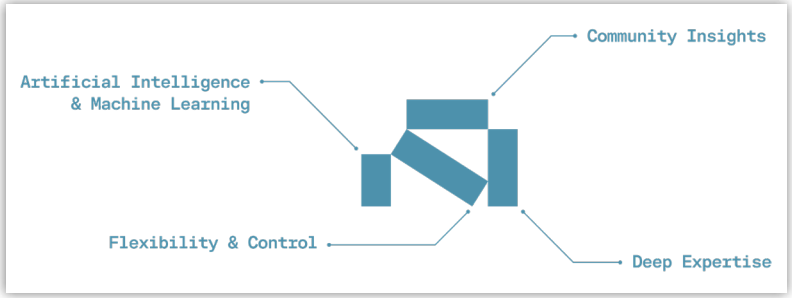
At a Glance:

- 3rd Party API Capabilities
- Professional Guidance/Services
- Fraud Engine/ Platform Functionality
- Payment Gateway Capabilities
- Operational Support
- Account/Client Management

Accertify 3D-Secure

Accertify serves your risk strategy and business objectives with:

- Artificial intelligence (AI) and machine learning
- Community insights from global network
- Significant level of industry knowledge
- Flexibility and controls that adapt to suit clients' needs



Unlike competitors offering black box solutions that rely solely on algorithms, Accertify's solutions balance the power of artificial intelligence with human intelligence.

Accertify 3D-Secure and Consumer Authentication

Regulators and card networks' requirements for stricter payment authentication to protect customers mean ecommerce businesses have increased pressure from multiple sides. Having an integrated payment and fraud risk strategy can help alleviate some of this pressure. **Accertify's** payment optimization solutions can help provide greater conversions and a better customer experience.

Accertify® Payment Optimization Solution

Accertify Payment Optimization solution enables merchants to develop intelligent 3D-Secure ("3DS") based decisioning globally to find the right balance between payment success, fraud liability and payment costs. **Accertify's** solution consists of three main modules: Strong Customer Authentication ("SCA") Optimization, 3DS Optimization and Risk-Based Authentication.

SCA Optimization

Strong Customer Authentication ("SCA") requires two-factor authentication on all ecommerce transactions that fall within the scope of the regulations. 3D-Secure is the preferred method of performing SCA, so its use is mandated for merchants. The use of 3D-Secure increases merchant processing fees and can lead to adverse payment conversion performance because of the friction imposed.

SCA exemptions provide scenarios where authentication and 3D-Secure can be bypassed, primarily due to the value and risk of individual transactions. Merchants and acquirer domains may request that the issuer grants an SCA exemption. Exemptions can be requested currently in the authorization message, bypassing 3D-Secure, or in the 3DS messages. Issuers either reject (soft-decline) or approve direct-to-authorization of exemptions, which will guarantee a frictionless experience for the consumer. Approved

Accertify 3D-Secure

merchant exemption requests, both via authorization and 3D-Secure, retain fraud liability with the merchant.

Merchant Fraud Strategy

Accertify believes that optimized usage of 3D-Secure and SCA exemptions are an essential part of a merchant's fraud strategy. 3DS not only brings financial benefits through fraud reduction and fraud liability shift, but it can also help to protect merchants' brands by ensuring customers feel secure when making purchases via app or website.

A complete and sound exemption strategy can contribute to a powerful uplift in payment conversion and customer satisfaction by prioritizing frictionless experiences. Finding the balance between fraud and friction should be considered a priority for merchants operating with the scope of SCA—a simple yet flexible integration where merchants keep control.

Accertify's SCA Optimization solutions allow merchants to create exemption strategies and comply with SCA regulations. **Accertify** can help to reduce costs associated with 3DS, reduce issuer soft-declines and improve payment conversion, all while maintaining a low fraud rate.

The solution can be deployed with minimal merchant-side development, as well as supporting a silent mode for performance monitoring ahead of deployment. The solution helps merchants take advantage of exemptions from SCA while preventing fraud. It assesses the key areas of compliance.

Accertify determines the location a transaction originates from and filters out the transactions that do not meet the scope requirements of SCA. Similarly, any payment type that is not in scope will be filtered out of the recommendation.

Using **Accertify's** Payment Fraud solution, a SCA Optimization solution can assess the fraud risk of an individual transaction and determine where it is safe to apply an exemption. This is considered relative to individual merchant's fraud risk and friction appetite, and it is completely customizable.

Lastly, the value of the transaction will be assessed to ensure it falls under the applicable limits which each merchant is able to apply exemptions. If multi-acquired, **Accertify** will provide routing recommendations to send an exemption request to the acquirer most likely to accept the exemption.

Use of **Accertify's** SCA solution has had previous success in attaining 99.98% frictionless rates alongside a 55% reduction in fraud cases.[1]

[1] Percentages based on M&S data taken in 2023 for the M&S Client Case Study.

Accertify 3D-Secure

SCA Optimization Issuer Profiling

Some merchants have concerns regarding the rate at which issuers in SCA regions soft-decline their exemptions. Soft-decline rates and reasons vary from issuer to issuer, and the merchant is not always able to understand why.

Issuer Profiling has the capability to profile each individual issuer's historic responses to merchant exemption requests. **Accertify** will provide merchants with an indication as to whether the issuer in question is likely to approve an exemption, or soft-decline it and send it to 3D-Secure accordingly. **Accertify** will recommend the best path to submit your exemption—authorization or 3D-Secure—at an individual issuer level, to ensure exemption approval rates and costs associated with 3D-Secure and soft-declines are optimal.

3DS Optimization

EMV 3D-Secure version 2.2 enables the merchant to request a "data share only" flow. This flow leverages the same 3D-Secure rails and data sharing; however, issuers are unable to challenge the transaction. This feature of 3D-Secure guarantees a frictionless checkout while uplifting authorization rates from between 7 and 12%[2] compared to direct authorization. This feature should be leveraged extensively in regions where 3D-Secure friction is a concern, such as the United States. Issuers in the US are conditioned to believe that 3D-Secure transactions are inherently high-risk. But by leveraging 3DS Data Share Only, merchants can safely send a greater portion of traffic to 3D-Secure, balancing their risk profiles, without the risk of transactions being disrupted.

Accertify's 3DS Optimization solution enables merchants to identify opportunities to use 3DS to improve authorization performance. Based on factors such as transaction risk, policy rules and individual issuer performance, **Accertify** can recommend not only when to use 3DS, but how to use 3DS for optimal performance – such as when to use data only flows.

High-risk transactions will likely be routed to an issuer-driven 3D-Secure flow, passing liability to issuers, whereas lower-risk transactions will be routed to Data Share Only. Additionally, **Accertify** will profile individual issuers across the globe to generate a view of which issuers have an acceptable success rate with Data Share Only. This view will also feed the recommendation.

Merchants can expect to realize the benefits to authorization performance of Data Only flows, compared to direct-to-authorization, identify high-risk traffic to relieve fraud liability and opportunities to reduce 3DS processing costs.

2. https://news.broadcom.com/tech-innovation/fewer-declines-more-approvals-arcots-3ds-pilot-proves-the-power-of-better-data

Accertify 3D-Secure

Risk-Based Authentication

For regions outside of SCA's scope, **Accertify** can provide dynamic risk based decisioning on 3D-Secure. They can also assist clients in developing custom 3D-Secure strategies that can differ based on distinct global regions. Merchants can expect to optimize their use of 3D-Secure, reducing unnecessary fees and friction.

Visa Acceptance Solutions, 3-D Secure

Depending on your business needs and integration requirements, **Visa Acceptance Solutions** offer several enhanced authentication solutions including 3-D Secure, Data Only, and more. Together with Visa's other subsidiary companies, Cybersource, CardinalCommerce and Verifi, Visa has access to the most modern, secure and optimized payment processes across the payment fraud and risk lifecycle.

Decision Manager plus Payer Authentication

With Decision Manager plus Payer Authentication, clients can use the latest 3-D Secure authentication. This additional layer of protection offers complete control over the authorization flow. Clients decide which transactions are sent for 3-D Secure® authentication processing before they're sent for authorization. This helps reduce chargeback rates and the need for manual reviews by blocking fraudulent transactions before they're sent for authorization.

Payer Authentication

Payer Authentication allows businesses to take full advantage of all the latest EMV 3-D Secure® authentication capabilities to improve their fraud performance without adding unnecessary friction to their payment experiences.

Businesses can collect and send additional data during the authentication process to help issuers determine whether a transaction fits the buying patterns of a specific cardholder and identify risky or fraudulent transactions. And easy integration with **Visa Acceptance Solutions** Decision Manager helps businesses quickly add Payer Authentication to their **Visa Acceptance Solutions** fraud management solution.

VISA Acceptance Solutions

At a Glance:

Outseer 3-D Secure™

Outseer, an RSA company, provides payment authentication, account monitoring and fraud management technology solutions to support secure growth of digital commerce. **Outseer** products and solutions have been built using identity-based science and machine learning to deliver high detection rates with little to no customer intervention, allowing for a more seamless user experience. **Outseer** processes more than 20 billion transactions globally, protecting more than two billion consumers each year.

Outseer 3-D Secure is a risk-based, card-not-present (CNP) and digital payment authentication solution mapping to the latest EMV® 3-D Secure protocol, the global standard for authenticating CNP and digital transactions. The protocol promotes a frictionless shopping experience for cardholders by leveraging risk-based authentication technologies, and it includes new transactional attributes that enhance the ability to distinguish genuine transactions from fraudulent ones.

Outseer 3-D Secure helps support Key Performance Indicators (KPIs), including:

- Increased transaction approval rates
- Improved customer loyalty thanks to a frictionless digital experience
- Reduced fraud losses
- Lower false-positive ratios

OUTSEER
An RSA Company

At a Glance:

Outseer chose not to participate in the Paladin Vendor Report at this time.
If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

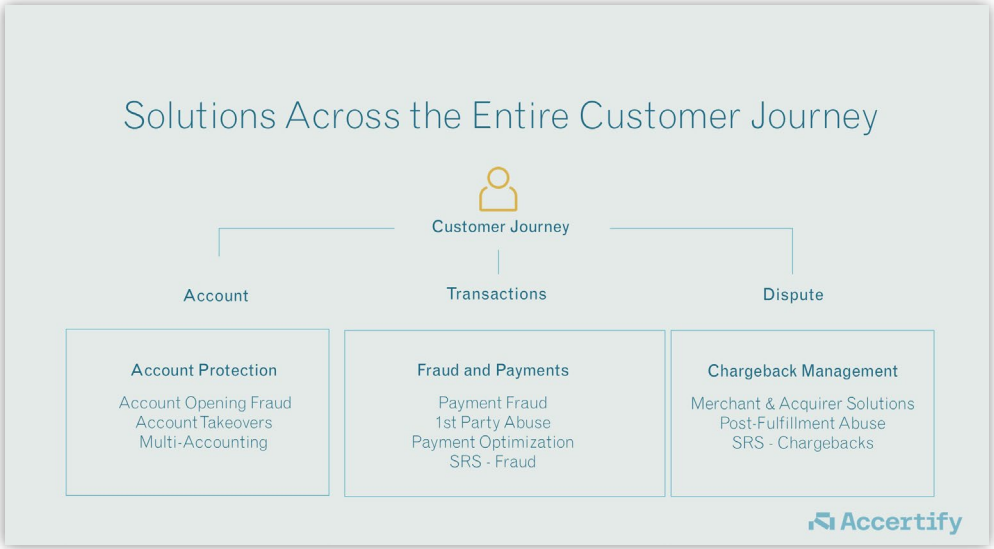
Fraud Platforms & Decision Engines

Third-party fraud prevention platforms provide protection and flexibility to not only prevent fraudulent transactions but also increase acceptance of legitimate orders. They help scale fraud teams by managing, or helping to eliminate, the manual requirement associated with transactional order review. Often, the foundation of the prevention platform is a customizable rules engine designed and maintained to identify historically high-risk combinations of order attributes, then make a decision on behalf of the merchant.

Accertify, Inc. ("Accertify")

Accertify understands that customer expectations are ever evolving and so is fraud. Today's online consumers expect to be recognized and rewarded as loyal customers. They want to transact with a single click from any device and feel confident their account is secure. At the same time, each online event exposes your organization to reputational and financial risks that can have a material impact.

Trusted by many of the largest companies globally, **Accertify** is a leading digital platform assessing risk across the entire customer journey, from account monitoring and payment risk to refund fraud and dispute management. **Accertify** built a comprehensive platform with integrated solutions across the entire customer journey, letting organizations see the complete picture and proceed with confidence. **Accertify** can help reduce the need to juggle multiple vendors and decipher fragmented risk scores that result in unwelcome friction for customers.



Accertify

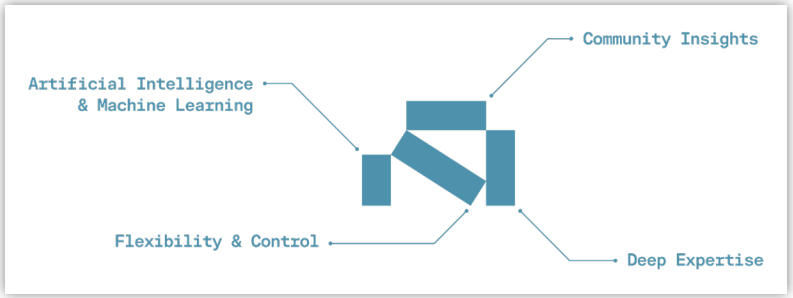
At a Glance:

- 3rd Party API Capabilities
- Payment Gateway Capabilities
- Operational Support
- AI Powered
- Account/Client Management
- Device Intelligence Capabilities
- Historical Sandbox Testing
- Professional Guidance/Services
- Fraud Engine/ Platform Functionality
- ATO Detection Capabilities
- User Behavior Capabilities
- Pre-Authorization Functionality
- Pre-Authorization Functionality

Accertify, Inc. ("Accertify")

Accertify serves your risk strategy and business objectives with:

- Artificial intelligence (AI) and machine learning
- Community insights from global network
- Significant level of industry knowledge
- Flexibility and controls that adapt to suit clients' needs



Unlike competitors offering black box solutions that rely solely on algorithms, **Accertify's** solutions balance the power of artificial intelligence with human intelligence.

Solutions and Functionality

The **Accertify** fraud platform is a software-as-a-service offering that allows clients to adapt their fraud-screening strategy in real time. It utilizes advanced artificial intelligence, machine learning models, configurable fraud and policy rules, and extensive reputational community data. The platform performs real-time risk assessments, and it offers a wide variety of pre-integrated connections to third-party data providers. **Accertify's** fraud platform includes core functionalities such as:

Machine learning powered by dynamic risk vectors: Machine learning capabilities power the creation of new predictive data elements for use in industry models. These elements capture community intelligence in a fundamentally new way, making it possible to:

- Identify consistency versus change across transaction elements to reveal threats
- Make dynamic updates to key data features as the risk grows or diminishes
- Use targeted community intelligence to bring additional knowledge to clients' transaction decisioning outside of their business interactions

Scoring: At its core, the fraud platform is a data management tool. By offering a rich set of integrated machine learning models, pre-built rules, and condition checks, clients can implement a range of policy checks to live alongside their fraud screening strategy. Designed for simplicity, the interface lets business users fine-tune risk parameters and evaluate outcomes.

Accertify, Inc. ("Accertify")

Case Management: The fraud platform offers clients a configurable tool that can be used to analyze data, assess risk, and report and manage fraud risk screening. While most of the traffic is managed via a machine-learning and rules-based approach, the case management system allows clients to build workflows that suit their team's structures and support their Service Level Agreements (SLAs).

Fraud & Abuse Prevention Highlights

2025 Highlights

- **Accertify** protected more than 10B transactions, worth over $1.2T USD.
- **Accertify** helped clients prevent 30.7M distinct fraud and abuse attempts worth nearly $5.8B USD in total attempted risk.

Based on Accertify 2025 client data.

2025 Cyber Week Highlights

- **Accertify** protected 107M transactions worth $12.9B in retail transactions alone.
- **Accertify** processed a peak of 2708 transactions per second.

**Statistics derived from Accertify client data from Cyber Five 2025 (Thanksgiving through Cyber Monday).*

Accertify Account Protection

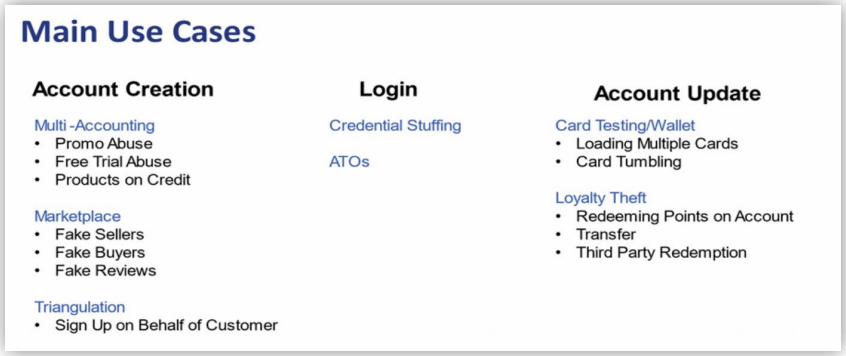
Recent data breaches have exposed billions of email addresses, passwords, and other personally identifiable information on the dark web. Malicious users harvest this data to execute sophisticated attacks designed to take over existing accounts or fraudulently open new ones. These acts are estimated to cost US firms over $5B annually[1]. To combat these problems, many businesses utilize several solutions to help prevent fraud, reduce loss, and enhance customer experience. However, juggling multiple vendors can be costly, can present a fragmented risk picture, and can introduce unwelcome friction for good customers.

Increasingly, businesses are choosing to partner with a company that provides an end-to-end solution across the entire customer journey. **Accertify** Account Protection monitors customer activity in environments with a focus on identifying risk associated with account takeovers (ATOs) and new account openings. The solution can detect loyalty account theft, bots, credential stuffing, promotional abuse, card testing, fake marketplace sellers, and other use cases, in real time.

Accertify Account Protection monitors each step of the user journey, from creating an account to logging in to making account updates. From the moment a customer enters the digital environment, Accertify Account Protection works in a frictionless

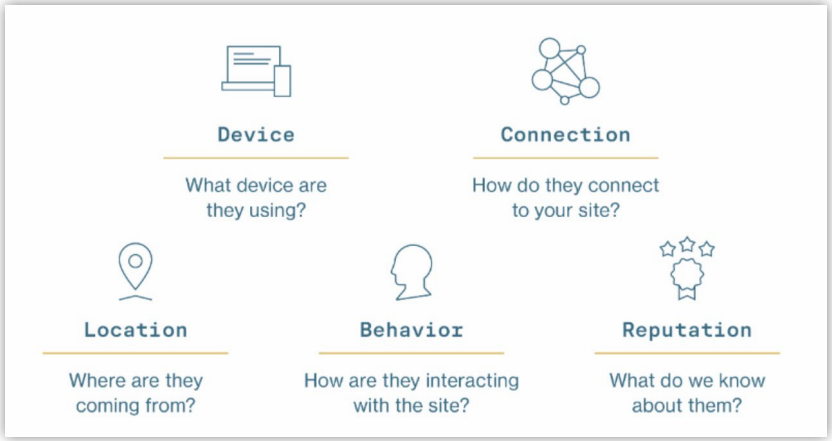
[1] https://securityintelligence.com/why-fraudsters-are-flying-high-on-airline-loyalty-programs/

Accertify, Inc. ("Accertify")

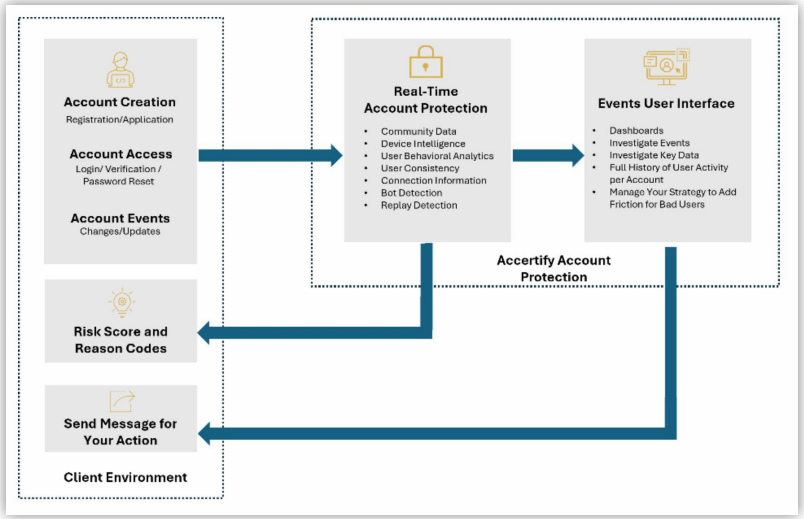


way to provide real-time end-to-end insights, distinguishing good from bad activity. **Accertify** Account Protection combines continuous monitoring and machine-learning algorithms to identify risky event activity when an event occurs, so clients can respond in real time.

Accertify Account Protection increases trust in an online transaction by answering these questions:



In addition, **Accertify** Account Protection provides a user interface, which allows clients to investigate suspicious activity and respond as they see fit.



Accertify Account Protection monitors data and behaviors about the user and returns a risk assessment that is based on device, behavior analytics, consortium insights, and historical comparisons to look for consistency and anomalies. **Accertify** Account Protection can detect sophisticated bots and analyze the intention of the bot to allow good bots and deny bots used to commit fraud.

Accertify, Inc. ("Accertify")

Accertify's model can detect sophisticated bots that present human-like behavior by looking at behavior replays across users, which would be impossible for humans to recreate. **Accertify's** machine learning solution can detect bot attacks in real time so you can take action automatically to mitigate the attack, while easily being able to report on the attack utilizing the attack sate signal offered on Account Protection's dashboard.

Accertify Account Protection Event Highlights

- Over 1.63B events protected, 49.7%YOY growth.
- Over 84.5 million high-risk events identified, including over 75.2 million risky logins.
- Client base grew by 24% YOY.

(Based on Accertify Client Data from 2024-2025.)

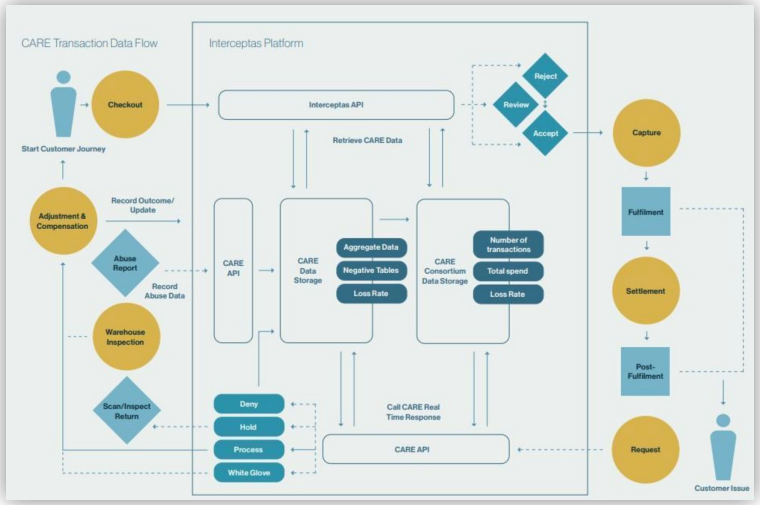
Accertify CARE solution (Claims, Adjustments, Returns, and Exchanges)

First-party fraud takes on many forms. **Accertify** has noticed an increase in users abusing and manipulating processes in order to profit from retailers' operational refund or policy loopholes. Many merchants lack the data needed to identify those who exploit their return policies or those who make legitimate purchases but excessive returns. To address these growing problems, retailers need a solution to help prevent abuse without impacting the experience for good customers.

Accertify's CARE solution is a purpose-built solution that collects customers' return data and allows merchants to monitor, measure, and take appropriate action in real time or to prevent future returns abuse. The **Accertify CARE** solution expands the capacity of the fraud platform to identify risks associated with post-fulfillment adjustments, such as claims, adjustments, refunds, returns, reshipping, and exchanges. The **Accertify CARE** solution provides current **Accertify** fraud platform users with a dedicated API and a unique endpoint to send post-fulfillment adjustments to transactions previously imported by the fraud platform.

Accertify's CARE solution gathers, stores, and analyzes transactions to produce an assessment of the level of risk of the CARE adjustment and evaluate whether to accept, reject, or manually review. **Accertify CARE** data is stored in a parallel virtual table and compared across multiple keys so that, when manually reviewing future transactions, the client can make efficient real-time comparisons between adjustment data and transaction data.

Accertify, Inc. ("Accertify")



Process Flow

Accertify Device Intelligence analyzes devices and associated identities transacting across digital channels via mobile applications and mobile and desktop browsers. The Device Intelligence platform helps clients verify identity, assess, and mitigate risk in real time while optimizing the customer experience.

A Software Development Kit (SDK) can be incorporated into mobile applications to access detailed mobile device information. More than a hundred device attributes and operating system attributes can be collected and analyzed to produce a persistent device identifier that is resilient to tampering, application uninstall/reinstall, and OS upgrade.

Core features include:

- **Malware and Crimeware Detection:** Analyzes connected devices to detect known malicious applications and criminal tools, such as location spoofing and IP address proxy apps. Malware files are dynamically updated without client interaction.
- **Rooted/Jailbroken Detection:** Protects against increasing—and increasingly complex —rooting methods used by fraudsters, such as cloaked root, through advanced root and jailbreak detection.
- **Trusted Path:** Security architecture prevents interceptions by providing a complete secure path to transport sensitive information, encrypted end-to-end, signed, and digitally protected against replay attacks. Trusted Path securely communicates sensitive messages.
- **Secure Messaging:** Secure means of delivering contextual two-factor authentication (2FA) messages to a registered device through the SDK and secure Trusted Path that cannot be read by any other device, intercepted, or replayed. This can be a stand-alone offering.

JavaScript collectors can be incorporated into any relevant web page to access detailed browser session information. Hundreds of attributes can be collected and analyzed to produce a persistent device identifier and identify potentially fraudulent behavior.

Accertify, Inc. ("Accertify")

Accertify's browser fingerprint "recipe" determines how well devices are differentiated from each other, allowing any client to seamlessly authenticate users with less friction by minimizing collision rates and maximizing fingerprint longevity.

Accertify User Behavior Analytics (UBA) offer clients the ability to track how their customers interact with the clients' environment using their UBA solution. By analyzing behavioral signals from users as they interact with client's websites, UBA can help distinguish good users from fraudsters and detect suspicious activity from humans or bots. The solution provides risk ratings and includes visual representations of a user's journey through a website, including measurements of length of time spent per page, mouse movement, keystroke dynamics, and pasting or auto-filling data into forms.

Accertify's enhanced link search functionality gives the client the ability to search for historic linkages that can clarify whether an event is out of pattern or is evidence of a loyal, repeat customer. The capability is flexible in what values can be displayed and searched and offers power users the ability to perform batch exports, execute data pivots, and bulk resolution capabilities.

Clients can test and simulate a condition or conditions using the **Accertify** Rules/Conditions Testing "sandbox." The functionality in the sandbox provides the ability to look historically and get an

analysis of a proposed rule change. For testing conditions on current and future transactions, a client can run tests in the production environment and set a passive score where it would not affect the outcome.

Accertify's Profile Builder identifies real-time patterns and trends through the dynamic summarization of data. Gives real-time insight at the transactional level to discern fraud rates, track new product launch limits, monitor account usage, analyze customer buying patterns, and uncover organized fraud rings. In real time, Profile Builder monitors summarized fraud rates at the product/SKU level, across airline route networks, at events/locations, against a specific entertainment genre, or any number of similar entities.

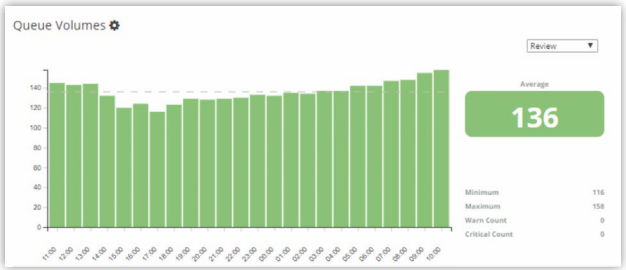
The complementary **Accertify Payment Gateway Module** is for clients seeking a singular platform for payments and fraud. The

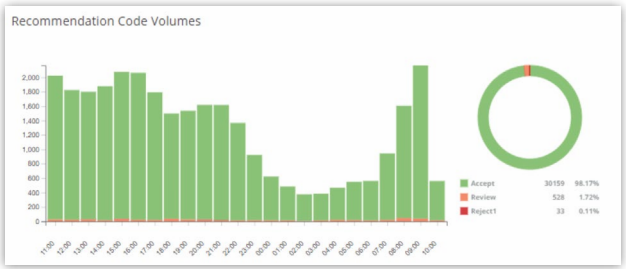
module is processor-agnostic, giving merchants the flexibility to select different processors for different payment types, and it provides easy connectivity to multiple acquirers globally.

Reporting:

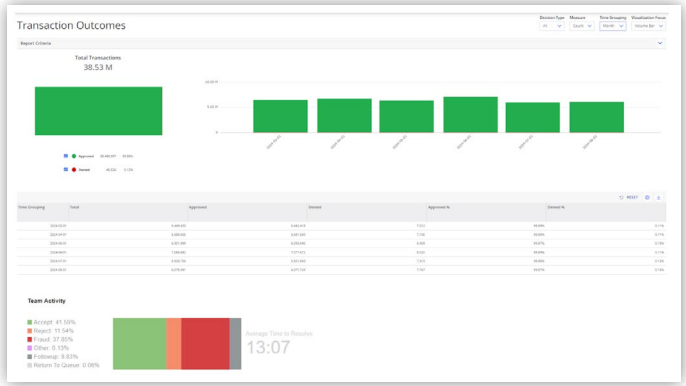
Accertify offers three types of reports.

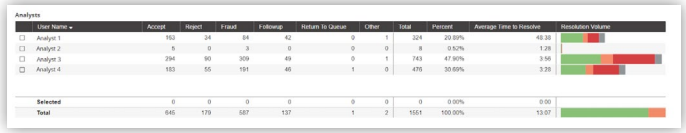
1. **A Landing Page Dashboard:** These are “heartbeat” views of platform statistics—including fraud, chargebacks, and performance—individually and across the team.



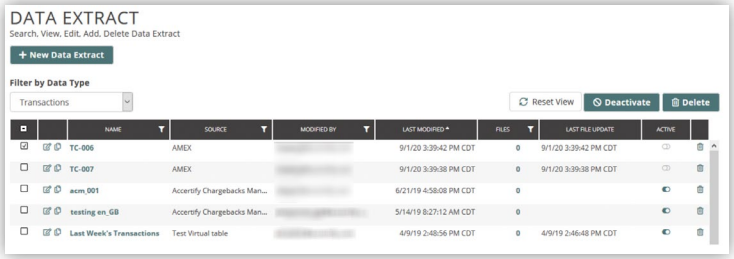


2. **Enterprise Reports:** These allow a client to input criteria parameters to specifically drill down and show different types of performance. Examples include monetary metrics, chargebacks, analyst decisioning, rules performance, and more.





3. **Report Builder:** This reporting suite allows clients to create either one-time or recurring scheduled reports where they can extract large amounts of data. Reports generated via the



Accertify, Inc. ("Accertify")

Data Extract Utility feature can be securely exported onto the client's systems where they can use their own software to look for trends or report to their own internal teams. More advanced features include data pivots and exports to Excel format.

Other Accertify Services Offered:

Accertify's global team of artificial intelligence and machine-learning experts and data scientists build industry-leading machine learning models, backed by **Accertify's** network of reputational community data to which some of our merchant clients consent to contribute. These models provide clear, defensible reason codes that detail insight into the factors driving the model decision.

Accertify's experts also provide client consultation, listening to clients' needs, sharing insights, and designing a set of machine-learning-based solutions. Their research and development focus on pioneering new machine-learning techniques, as well as analyzing new data streams to provide clients with new data insights and predictive risk behaviors.

A global team of Client Success Managers are responsible for assisting each client in achieving their fraud and chargeback goals. This team is primarily composed of former fraud-prevention leaders for the most recognized brands in the world and possess extensive first-hand fraud and chargeback experience. Client Success Managers have a deep understanding of the **Accertify** Fraud and Chargeback Platform and understand how it can be deployed to solve complex challenges. The team stays closely aligned internally to ensure clients are aware of new features and functionalities.

Through Strategic Risk Services, the team provides direct operational management of a client's fraud and/or chargeback processes through the fraud platform. They become an extension of the organization by providing experienced and comprehensive consultation, geographical coverage, and SLA management.

A dedicated Support Services team stands by. By completing rigorous platform and technology training, **Accertify's** multilingual team's extensive fraud prevention, chargeback management, and client success experience ensures success. In addition, through a secure web portal, they offer a set of user-friendly support resources to further support clients.

Finally, **Accertify** offers a wide range of professional services designed to help clients optimize fraud prevention, chargeback management, and payments performance. The Professional Services team brings years of industry expertise and know-how as former fraud and chargeback managers, Certified Fraud Examiners, online technology experts, statisticians, and professional trainers.

Visa Acceptance Solutions

Visa Acceptance Solutions offers automated and customizable tools that enhance fraud prevention and revenue control. Their advanced AI-driven models, backed by Visa's secure network, deliver strong risk management that improves over time with billions of processed transactions from both **Visa** and **Cybersource**.

Core Capabilities

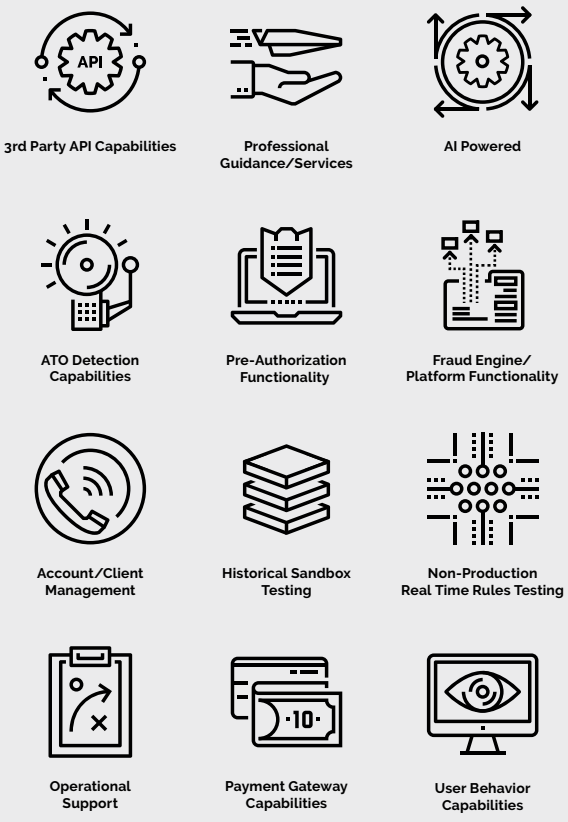
Visa Acceptance Solutions offers two core products: Decision Manager is designed for enterprise businesses, while Fraud Management Essentials is for small and medium businesses. These solutions apply advanced AI-powered fraud management capabilities, using actionable intelligence and machine learning-driven risk models to automate decision-making, balance risk and revenue, and enhance customer experience.

At the foundation of **Visa Acceptance Solutions** is a modular platform that uses a unified set of APIs, allowing seamless integration with any system across various industry verticals, such as retail, ecommerce, transit, telecommunications, restaurants, airlines, insurance, and utilities. This flexible platform supports the deployment of highly configurable rules and automated strategies tailored to specific business needs, enabling organizations to harness the full power of Visa's secure network and advanced AI for comprehensive risk management.

With the acquisition of Featurespace, Visa Acceptance Solutions offer acquiring risk solutions, and transaction management tools to detect fraud and manage risk throughout the entire payment lifecycle to support their merchants.

VISA Acceptance Solutions

At a Glance:



Visa Acceptance Solutions

Automate your fraud decisions with AI:

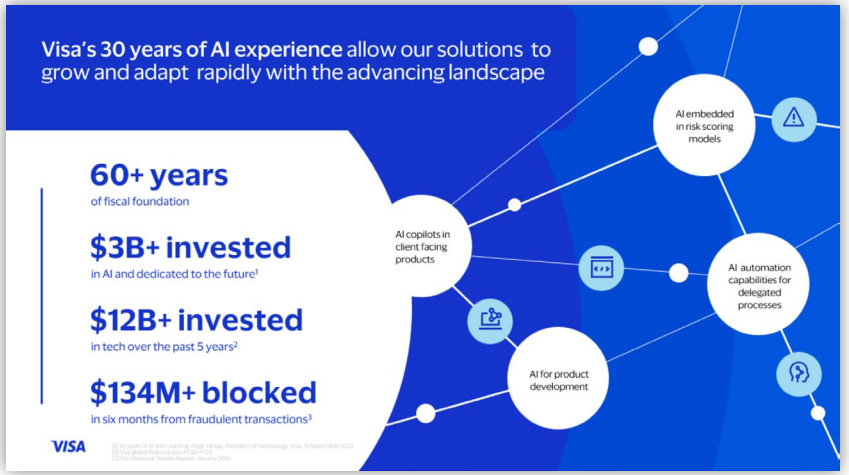
- Create a complete risk strategy based on a transaction's risk score—don't limit fraud detection to one rule; instead, use highly configurable rules to meet specific needs.
- Set up scenarios and instantly anticipate outcomes of your new risk strategies to verify they are effective before going live with Decision Manager Replay.
- Only 0.78% of transactions required manual review following Decision Manager screening[1]
- 99% of transactions are good.[2] Their AI is trained to help recognize good customers through Identity Behavior Analysis and to help maximize revenue capture[2].

Shift the focus to accepting more good customers:

- An innovative AI-powered Identity Behavior Analysis risk model automatically helps identify good transactions or reject bad transactions based on your customer's behavior indicators. You'll get a score that verifies their validity.
- It can improve decisions and help avoid false positives. It also helps provide a better customer experience for good customers who don't have to be screened for fraud.

Increase acceptance rates with real-time, flexible strategies:

- When a customer makes a purchase, Decision Manager's customization options, machine learning, and billions of data points come together nearly instantaneously to determine the validity of the transaction. Without waiting for status timers, instant decisions drive a smoother customer experience.
- Decision Manager not only provides you with the insights needed to accept more valid orders but also gives you the flexibility to design a strategy that suits your specific business needs.



[1] Calculated as the percentage of transactions screened by Decision Manager in FY25 that required manual review.
[2] Based on data collected from Decision Manager platform in FY25. The fraud rate for all transactions across Decision Manager is 0.5%
[3] Machine learning algorithm is based on Visa transactions (276B) + Decision Manager transactions + third-party data partners' transactions

Visa Acceptance Solutions

What makes Visa Acceptance Solutions different

Machine Learning & Artificial Intelligence

Based on more than 276 billion transactions annually[3], the artificial intelligence engine consists of multiple constantly evolving neural networks interlocked to assess active behaviors without the need for manual intervention.

KPI Dashboard

Gain instant access to real-time KPIs, empowering the end user to swiftly identify emerging trends, detect anomalies, and monitor overall performance with precision.

Powerful Searching

Experience enhanced search capabilities with extended date ranges and dimensional searching, enabling more powerful and comprehensive data retrieval.

Fraud Strategy Manager

Use continuous monitoring to proactively identify issues and enable users to develop and enhance their fraud strategy in alignment with their business priorities.

Automated Case Manager

Use AI-driven automation to streamline and optimize manual review processes, significantly reducing operational workload.

Expanded Coverage

Visa is evolving to help protect more revenue with enhanced support for new payment types, single-message gateways, and flexible API fields that enable even stronger fraud strategies and risk scoring.

Policy Abuse

Effectively manage refund and loyalty abuse with advanced fraud screening techniques, integrated with the rest of your fraud strategy.

Network

Extremely high rate of uptime and stability come with the global reach of Visa and Decision Manager transactions.

Identity Behavior Analysis

Cybersource's positive behavior AI focuses on the 99% of transactions that are valid[4]. Identity Behavior Analysis uses historical customer identity information across different sellers and industries by using machine learning to automatically identify good, bad, and never-seen-before customers.

[4] Based on data collected from Decision Manager platform. The fraud rate for all transactions across Decision Manager is 0.5%.

Customization

Highly refined customization allows businesses to fine-tune their fraud strategy to their chosen level of detail.

Digital Device Identity

Capture both device fingerprint and behavioral biometrics to accurately identify fraud.

Transparent Decisions

Decision Manager offers full insight into the reasons why a decision was made, not just the score, and puts the user in control. Tools like Decision Manager Replay create a low consequence environment for merchants to review and test new strategies without impacting the customer experience. Merchants can create a complete risk strategy based on a transaction's risk score and configure for their business scenarios.

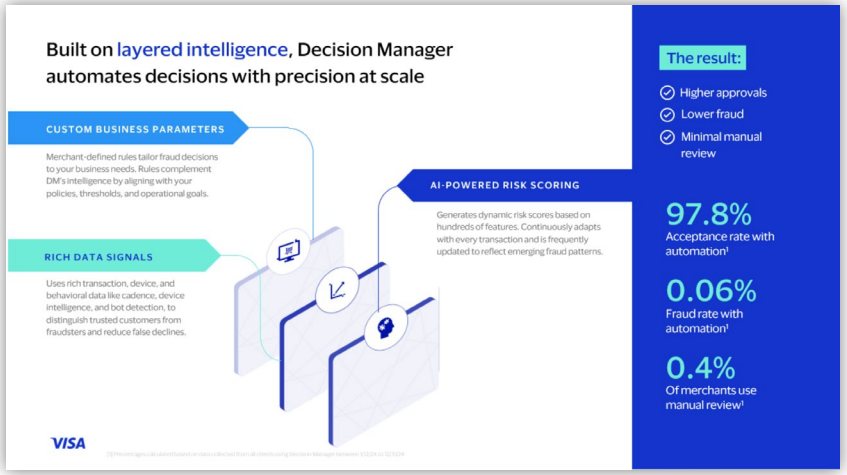
Transaction Management

Get direct access to review and investigate individual transactions. Discover the links between positive and negative transactions with Decision Manager's visualization options.

A complete suite of risk and fraud management solutions

Decision Manager

With AI at its core, Decision Manager integrates AI-powered risk scoring, dynamic identity signals, and tailored business parameters, delivering enhanced customization and control. This layered approach helps support fraud decisions that are fast, scalable and "context-aware," adapting to real-world behavior, evolving threats, and the nuances of each business environment. By combining predictive models with behavioral intelligence and merchant-specific logic, Decision Manager enables smarter approvals, fewer false declines, and a more seamless customer experience. Together, these elements help create a fraud solution that's not only intelligent, but also deeply aligned with each merchant's reality.



Fraud Management Essentials

Fraud Management Essentials is the small and midmarket fraud solution of choice. With ready-to-go fraud filters, businesses can automatically monitor transactions while still providing seamless

customer experience. It's a streamlined and powerful fraud prevention tool to prevent common attacks such as card testing, payment fraud, and common abuse scenarios. Built on the same machine learning network as Decision Manager, Fraud Management Essentials utilizes powerful risk models and hundreds of validation tests to automate detection and prevent fraudulent transactions. Setup is streamlined, with preconfigured settings that make it simple to start and make informed decisions via a user-friendly dashboard.

Global Identity Services

In addition to the Visa and Cybersource data networks, Decision Manager clients can further strengthen the power of their machine learning with additional behavior signals and risk scores from third-party providers already integrated into the platform. Clients can choose from a marketplace of data providers specific to their industry or business needs, and benefit from their data with no additional IT cost.

Account Takeover Protection

Account Takeover Protection helps prevent account takeover and other pre-transaction attacks through fully customizable strategy options.

Watch List Screening

Watch List Screening offers real-time screening to globally sanctioned and denied parties lists. This provides knowledge to make informed decisions about denied parties, even to businesses not required to connect to these lists by regulation.

Delivery Address Verification

Delivery Address Verification can help reduce the shipping and customer service costs for a business by detecting and fixing errors in real-time.

Payer Authentication

Visa-enhanced Payer Authentication manages the customer experience with an end-to-end authorization flow and provides an additional layer of protection with 3-D Secure authentication.

Verifi Post-Purchase Solutions

Verifi solutions help merchants prevent and resolve disputes with the use of compelling evidence, data transparency, and merchant-initiated or rules-based refunding globally. Verifi equips merchants, issuers, and acquirers to reduce financial losses, create operational efficiencies, and remove unnecessary fraud and first-party misuse disputes from the payment ecosystem.

Experience & Expertise

Visa Managed Risk Services

Visa fraud and risk management solutions are supported by experts with extensive experience, and merchants can choose to work with a Visa Managed Risk Consultant for personal expertise

and support. With highly experienced consultants around the globe, **Visa Managed Risk Services** provides businesses with expert support that can further enhance fraud management strategies.

Organizations that partner with Visa Risk Consultants are provided with a fraud chargeback rate and a Decision Manager acceptance rate that supports alignment with the business's goals, increases revenue, and reduces customer friction.

Pricing Model

A variety of pricing options are available to merchants, which can be influenced by transaction and sales revenue criteria. Supplemental fees may be applicable depending on region, acquirer, and processor requirements. **Visa Acceptance Solutions** offer services and tools to help optimize revenue and minimize fraud based on business needs and goals.

Planned Updates and Enhancements

Products and components may be updated and enhanced on an ongoing basis based on a combination of user feedback, usability research, fraud landscape knowledge, and opportunities for innovation.

Experian

Experian Identity and Fraud Solutions serve a range of verticals, including ecommerce, fintech, marketplace, and financial services. The solutions are classified into four categories: identity verification, fraud analytics, step-up verification, and workflow orchestration.

The solutions utilize **Experian**-owned consumer data, commercial entity data, device intelligence data, and a network of specialized partner solutions that cover a range of alternative data, email intelligence, phone intelligence, and behavioral analytics signals. The platform makes it possible to combine data assets to meet use case requirements—and to orchestrate in a way that optimizes performance and limits costs.

The platforms handle over 6 billion transactions annually operating within omnichannel, online, in-person, and call center environments using API, UI, and batch-based access as customer needs and use cases dictate.

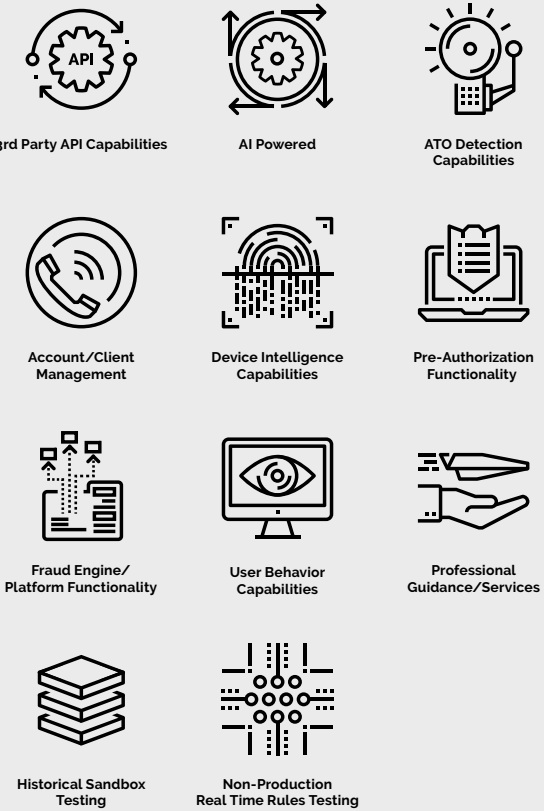
Experian Identity and Fraud solutions focus on five primary client needs:

- Customer Experience
- Growth
- Risk/Loss
- Cost
- Compliance

Solutions and Functionality:

The Ascend Technology Platform™ was built to give clients full control over their identity and fraud rules and strategies through a browser-based User Interface (UI). **Experian** identity and fraud personnel partner with the client to build the initial ruleset, models,

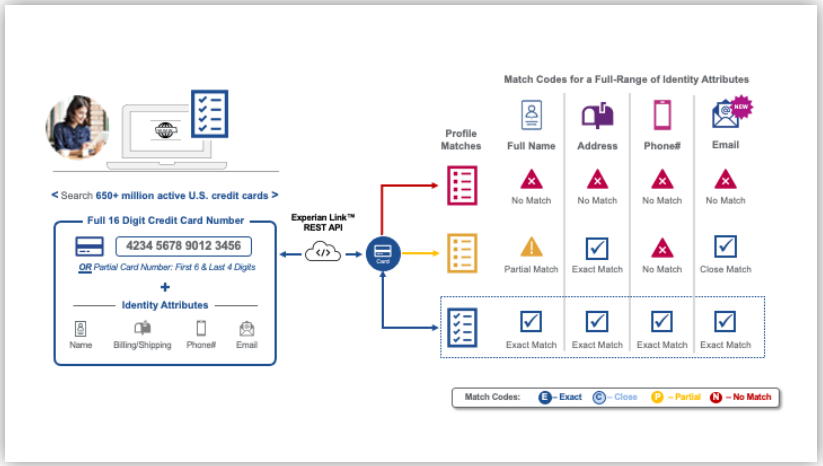
At a Glance:



and analytics to meet client's requirements for identity verification, fraud risk management, and authentication as well as applying **Experian's** expertise. Subsequently, the client can modify that ruleset through the UI, which doesn't require coding, nor does it require any paid engagement with **Experian**. Here, the client can manage and control their own rules as needed.

Orchestration rules dictate which **Experian**-driven solutions are included for each use case or transaction for identity verification, fraud risk management, and authentication. This includes when to use a solution (logical conditions are applied), the order in which solutions are used, and whether solutions are called in parallel or sequentially. Additionally, this includes cases in which an event needs to be paused and resumed due to a required offline process (step-up authentication, for example).

Strategy rules take all the information gathered through the orchestration steps to determine a final, optimized, and combined outcome for the event. The orchestration rules may dictate that several solutions are called for an event, but the strategy combines the attributes and outcomes from those solutions into one overall decision. The platform response returns all the individual attributes and outcomes along with a singular, overall outcome. Any rule-related capability of individual backing solutions remains unaffected by Ascend, so those can offer additional ways to control the outcomes of individual solutions.



Experian Link enhances credit card authentication for the merchant by linking the payment instrument with the digital identity presented for payment. This service matches each identity attribute presented by the consumer with attributes on file with the card issuer and enhanced attributes across **Experian's** network.

Experian Link responses are used internally as part of client's fraud models. No rules are defined out of the box, but benchmarks for decisioning are part of use case recommendations. The functionality can help support risk management at the following user interactions:

- **Account creation and checkout:** Increase trust by helping verified customers sign up and check out quickly and securely
- **Changes to existing accounts:** Prevent account takeover by assessing updates to existing delivery or contact information.

Experian

- **Batch analysis of cards on file:** Proactive card on file portfolio analysis, monitoring, and flagging to purge bad actors from your ecosystem
- **Frictionless balance transfer check:** Verify credit card ownership passively for low-risk operations before performing a balance transfer without kicking-off FCRA requirements

Reporting options available:

Experian solutions offer performance and management reporting capabilities. The preconfigured reports help users manage the day-to-day operations and understand the impact of decisions in terms of approvals, refers, and pends to optimize fraud capture rates, customer experience flows, and growth. Self-service capabilities are also available as a premium offering to enable direct access to the databases for more sophisticated and custom reporting for clients.

Proof of Concept process:

Historical and real-time validations are available to provide proof of concept using the activity with known outcomes depending on customer needs and use cases. However, this does not pertain to solutions that require the client to provide data captured during an online interaction, such as the attributes from a digital device or online behavior that cannot be recreated after the event has occurred.

Pricing format:

Experian Identity and Fraud Solutions support a range of pricing options depending on customer needs and use cases. Examples include:

- Flat fee
- Transaction-tiered based
- Monthly min
- License-based

Integration options available:

Experian's Identity and Fraud solutions offer a wide range of integration options. They connect directly to the platforms using a JSON-based API and access solutions through a web UI. They also connect through platforms and services offered by other **Experian** business units as well as those provided by a broad array of third-party integrations and other services.

Experian Link's real-time API integration can be done in as little as a week, with minimal effort from clients. Time from contract signature to go-live is as little as one month, depending on client UAT and contractual process.

White-label options are available, and third-party integration partners include loan origination, payments, and other providers. Backing partners deliver niche capabilities that include email

intelligence, phone intelligence, behavioral analytics, alternative consumer information, document verification, and international consumer data.

While SLAs can be negotiated with clients, the general uptime goal is 99.9%. The starting points for products and actual performance and response times can vary by product and product option. Currently, the monthly average is under 1 second across the 2000+ identity and fraud clients with certain clients running in sub-second response ranges.

Available Support:

Experian's Performance Monitoring Team proactively monitors for exceptional changes in existing implementations daily, including volume changes and key KPI changes. Additionally, the Experian team meets with clients at regular frequencies to review performance and discuss tuning observations with the client.

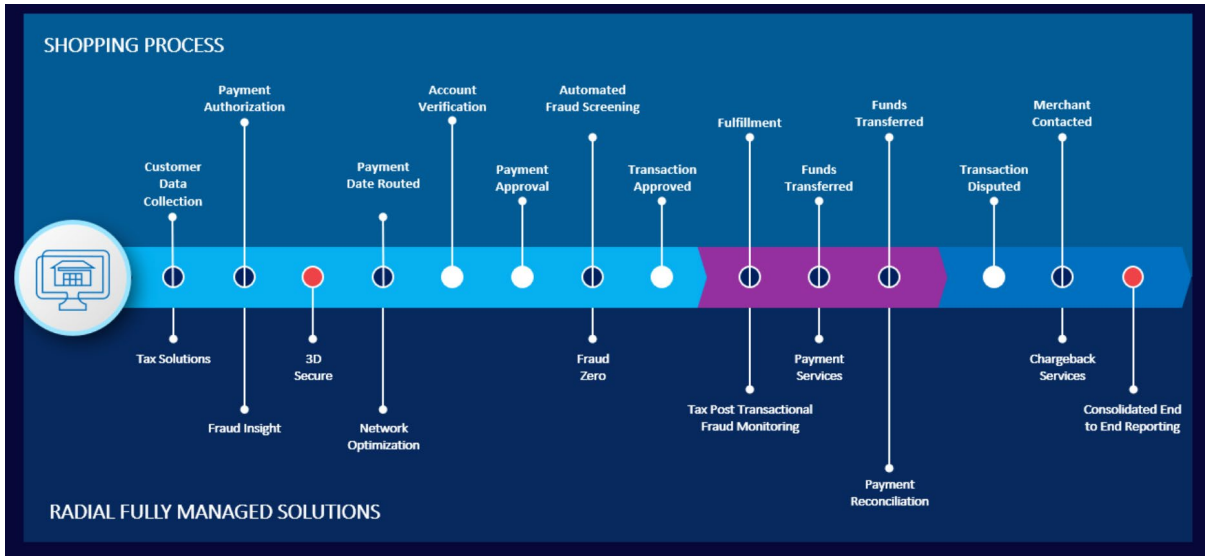
12-month roadmap initiatives are focused on three key areas:

- Continued enhancement to identity resolution and fraud predictiveness through additional data sources (internal and external), coupled with advancements in analytics around machine learning, AI, attributes, and triggers. This includes giving clients access to data and attributes in a self-service sandbox, creating signals, and enhancing fraud detection capabilities to reduce false positives and drive better customer experiences and outcomes.
- Authentication enhancements provide clients with an increased number of choices to meet business needs. This includes an emphasis on more passive tools like behavioral analytics and continued enhancements to present appropriate amounts of friction, such as document capture. For Experian Link, enhancements to PII component matching will include email and IP addresses as well as all-out scores for different combinations of PII.
- Identity and fraud exchanges will help clients build consortiums to share data in a permissible manner and drive better fraud decisions, eliminating known bad actors as soon as possible from the ecosystem and reducing friction for good users.

Radial Payment Solutions (RPS)

Radial Payment Solutions (RPS) protects commerce transactions throughout the customer's journey from initial discovery, purchase, return (for ecommerce), social, and point-of-sale channels. The solution provides a unified approach that mitigates fraud, resulting in protected revenue, trustless customer interactions, and growth. For more than 25 years in the ecommerce industry, **Radial Payment Solutions** has been managing fraud and payments for some of the largest ecommerce brands.

Modular by design, their integrations let the client select the best configuration that fits the immediate needs while keeping a number of options open for future expansion. This allows users to select from the Fraud Solutions, Chargeback Services, and Payment Services individually or as a group to maximize the benefit of a leveraged solution for ecommerce and in-store transactions.



Radial
powering bpostgroup

At a Glance:

- 3rd Party API Capabilities
- Payment Gateway Capabilities
- AI Powered
- Guaranteed Chargeback Liability
- ATO Detection Capabilities
- Account/Client Management
- Device Intelligence Capabilities
- Historical Sandbox Testing
- Non-Production Real Time Rules Testing
- Pre-Authorization Functionality
- Professional Guidance/Services
- Operational Support
- Fraud Engine/ Platform Functionality

Radial Payment Solutions (RPS)

RPS Fraud Services

RPS's Fraud Services provide zero liability against fraud. These services include pre- and post- authorization capabilities as well as complete chargeback management services. In addition to zero liability against fraud, they provide custom service level agreements to ensure clients achieve the expected results.

Pre-Authorization: Fraud Insight

RPS Fraud Insight, **Radial's** pre-authorization service, provides streamlined processing of individual shopper transactions and helps block unwanted and costly fraudulent transactions. Fraud Insight integrates with several third-party APIs to bring network-level rule development capabilities that build customized, unique targeted solutions to fit a client's specific shopper profile and behavior.

Radial helps focus on identity and intent of the transaction—utilizing behavior, historic, and real-time data to develop metrics that can be used in a split second to positively identify an unwanted attempt. One common use case for pre-authorization is card testing. Fraud Insight is adept at eliminating this type of transaction using velocity rules, which can be adjusted to fit seasonal and unique merchant-driven events.

In addition to card testing and other common cases, **Radial** builds specific use cases from consortium data that can adjust to changing fraudulent tactics. They are continuously monitoring transaction flow and utilizing machine learning, large language models (LLMs), and proprietary data training sets to predict and implement more effective strategies.

With Fraud Insight, organizations can get instant, cost-effective access to advanced fraud detection algorithms, machine learning, artificial intelligence, real-time monitoring capabilities, and valuable consortium data that can identify emerging fraud patterns and proactively respond to new threats.

Post Authorization: Fraud Zero

RPS's Fraud Zero service is Radial's comprehensive post-authorization product providing **fraud screening** to protect transactions after payment authorization. In developing the real-time fraud engine, they utilize various methods of machine learning, large language models, and proprietary data training sets to predict and implement more effective strategies. In addition, their proprietary device-fingerprinting software contributes to a universal data profile that can then be utilized to rapidly determine customer identities and intent.

Radial Payment Solutions (RPS)

Fraud Zero is specifically designed for merchants who want to remove the burden of fraud management, while benefiting from higher order conversions that drive revenues. It applies sophisticated fraud detection and management tools to deliver complete fraud screening and order acceptance.

By integrating several third-party APIs, expanded data provides network-level rule development capabilities to build customized, unique targeted solutions to fit a specific customer profile and behavior. Their models incorporate current transaction attributes and over 8 billion historical records—resulting in hundreds of data points being evaluated to produce a block or allow decision with a sub-second response time.

All these data points allow **Radial** to build targeted solutions for specific types of fraud attempts like Account Takeover (ATO) fraud, which has grown across all of ecommerce in recent years. Attack vectors for ATO are varied and specific for each merchant customer journey. **Radial** works with an organization to identify and mitigate these attempts—not just one time, but throughout the year as the threat arises.

With **Radial Fraud Zero's** brand protection, merchants can offer a reduced friction experience to valued customers, while preserving the reputation of the retailer. Brand protection capabilities include:

- Configurable purchase thresholds
- Customizable SKU monitoring
- Specialized monitoring for sales and promotions
- Automatic order cancellation when limits are exceeded

RPS Payment Orchestration Services

RPS Payment Orchestration Services provides the ability to process payments directly through the **Radial** platform for ecommerce, social, and in-store transactions. This consolidation ability delivers:

- Robust reconciliation and risk management processes across channels
- Volume-based pricing from gateway processors and acquiring entities
- Transaction routing to multiple payment networks and gateways

Radial maintains direct relationships with payment providers and, through their comprehensive API interface, make integration relatively seamless for the client.

Orchestration Services includes the ability to remove any transmission of credit card data from a merchant's workflow. Beyond tokenization our (SF) Secure Form technology creates a secure channel of communication between the shopper's browser

and **Radial** servers. This reduces the merchant PCI DSS scope to the lowest level possible for accepting ecommerce payments.

Their 3DS solution is a security feature that can be added to the overall fraud strategy. The **Radial** 3DS solution supports EVM 3DS2. As a part of pre-authorization, a transaction that triggers a 3DS call will be sent to the issuer of a shopper's card for authentication. The issuer can then request the shopper to verify their identity or not. Either way, when a transaction is authenticated through 3DS, issuers provide a liability shifting benefit for that transaction. **Radial's** 3DS solution can be customized for transaction size and other attributes to maximize the benefit of this standard and then minimize shopper checkout friction.

Chargeback Services

RPS's Managed Chargeback Services is a fully outsourced and fully integrated service organizations can utilize alone or in conjunction with the Payment Gateway or Fraud Solutions. **Radial** incorporates automation of chargeback notifications from processors, shipping details, and documentation from order management systems. Added to relevant data from customer service platforms, they can then streamline the review and minimize response time during any season.

Radial can consolidate differentiated chargeback process requirements from the Networks (Amex, MasterCard, Visa, Discover) as well as alternative payment providers (PayPal, Klarna, CashApp) to give the organization a true universal view of chargebacks across payment methods.

Radial partners with external vendors to enhance the pre-chargeback notification process to manage dispute deflection and alerts. This saves money and time. Their chargeback service is fully integrated to the Fraud Solutions, creating a leveraged benefit for fraud prevention. However, they can also work with third party fraud solution providers for client dispute management needs.

Radial monitors all network chargeback regulations and threshold requirements to keep clients informed of changes and actions that must be taken to be in compliance and provide guidance on balancing checkout optimization with best practice recommendation on return policy and other terms and conditions.

Onboarding / Account Management

Depending on the services being integrated from **Radial Payment Solutions**, they start with a consultative approach to provide a review of current capabilities and future needs. They have a dedicated team of payment, fraud, and chargeback specialists

to assist in evaluating what solution would work best and how to prioritize options. For instance, depending on demographic and product risk profile, they may recommend that different Buy Now Pay Later solutions be added to a payment mix. For their Fraud Solution, **Radial** will provide a historical analysis of transactions to launch with an effective strategy starting on day one.

Depending on the internal development team's resources, a typical integration timeline for all Fraud Solutions, Chargeback, and Processing Services (ecommerce) takes 6-8 weeks. In-store processing rollouts are highly dependent on store footprint and point-of-sale software needs. Clients can integrate directly with APIs or through several pre-built integrations with the major ecommerce platforms including Adobe Commerce, Salesforce Commerce Cloud, and Shopify.

Post launch, clients will be managed by a dedicated account manager. This results in a single point of contact for all communication with **RPS**. This management includes 24/7, 365-days-a-year technical support services that monitor performance and can respond to issues as they arise at any time. **Radial** proactively schedules monthly and quarterly business reviews to review results and provide information on the industry and trends for payments and fraud.

Pricing format

A number of payment options based on the platform elements exist. These include:

- Flat fee
- Transaction-based
- Payments (pass through)
- Fraud (Percentage based on Cost Of Goods)
- Chargebacks are included complimentary with a full Payments & Fraud Solution
- Fraud Solution can also be priced on a per-transaction fee

Roadmap priorities for 2026 include:

- Agentic Commerce
- AI Insights
- Returns Abuse Intelligence

Riskified

Riskified empowers businesses to unleash ecommerce growth by taking risk off the table. Many of the world's biggest brands and publicly traded companies selling online rely on Riskified for guaranteed protection against chargebacks, fighting fraud and policy abuse at scale and improving customer retention. Developed and managed by a large team of ecommerce risk analysts, data scientists, and researchers, **Riskified's** AI-powered fraud and risk intelligence platform analyzes the individual behind each interaction to provide real-time decisions and robust identity-based insights.

Benefiting from a sizable team dedicated to researching global fraud and training machine learning models, the platform analyzes the individual behind each interaction to provide real-time decisions and robust identity-based insights. The platform reviews shoppers and transactions across its global merchant network.

Riskified's platform is relevant to any large enterprise accepting online payments globally. The organization supports customers in a wide range of industries including diversified online retail, luxury fashion, home goods, electronics, travel, ticketing, remittance, gaming, food delivery, online marketplaces, and others.

Solutions and Functionality:

Chargeback Guaranteed Fraud prevention:

Riskified's chargeback guarantee solution provides instant decisions as well as automated representment support in conjunction with full chargeback protection. The machine learning models analyze hundreds of features per transaction, generating "approve" or "decline" decisions with sub-one-second response times. With nearly a decade of Chargeback Guarantee decisions having taken place on the platform, every

At a Glance:

decision draws on over a billion prior transactions processed for global ecommerce organizations across industries.

The machine-learning-supported functionality first collects and enriches transactional data in order to make a decision. Once the decision is made, transactions are reviewed to ensure that they are tagged correctly—and to identify anomalies among larger trends. The end-to-end process provides built-in methods to ensure that models stay fresh and decision making improves.

In addition, the platform provides context for every decision and provides support teams and fraud teams with dedicated tools. Agents and leadership can use the provided Control Center to track performance or dive into the data to analyze fraud and payment trends.

At the time of onboarding, **Riskified** analysts support every account by adjusting models and segmentation to optimize performance for each merchant.

Policy Protect:
For organizations offering programs such as rewards, friends and family discounts, referral discounts, etc., policies are typically established in attempts to prevent abuse of these programs. However, malicious users commonly attempt to abuse such policies to their benefit. **Riskified** offers protection from such abuse, as well as refund, promo, and reseller abuse.

The primary challenge in this instance is the balance between preventing abuse and maintaining customer experience. **Riskified** utilizes network data to cluster accounts together in order to reveal patterns of abuse. Through the process, organizations can get a better sense of what groups of orders to block and mark as suspect and which transactions can safely be accepted.

Identity Explore, enhances Policy Protect's capabilities by allowing merchants to visualize customer identities and behavior, tailor customer experience, and customize policy decisions. A high-resolution visualization of **Riskified's** identity engine, Identity Explore gives merchants the ability to analyze, investigate, and interact with customers on a whole new level. Through this offering merchants are empowered to optimize, and ultimately personalize, their policies.

Dispute Resolve:
Dispute Resolve allows merchants to simplify their chargeback management operations with a single smart platform.

With **Riskified** integrated into your checkout flow, every order's contextual data is collected and enriched. If it comes back as a chargeback, that data is leveraged to compile the best evidence and boost your chances of success.

Chargeback workflows differ depending on what, where, and how you sell. Dispute Resolve can automate as much or as little as you

desire, allowing you to maximize efficiency while retaining as much control as you need.

Riskified integrates directly with your gateway to fetch chargebacks and disputes in real-time.

Account Secure:
When fraudsters gain access to good customers' accounts, they cause damage that extends well beyond chargebacks. In an ATO attack, private customer data, loyalty points, and stored payment methods are compromised. Most importantly, account owners blame the merchant for failing to protect their account and are likely to reduce their future spend with this merchant—or even churn entirely.

In addition to analyzing device and behavioral factors, Account Secure's accuracy is largely fueled by **Riskified's** expertise on the transaction level. Each login and account event is linked to historical transactions both at this merchant, and across their network.

Reporting options available:
Riskified Chargeback Reporting view provides aggregated chargeback reimbursement and dispute stats in the Control Center dashboard, and offers granular data so users can track reimbursements and disputes on the order level. This allows merchants to easily track **Riskified's** performance and gain insights into chargeback populations. Users can analyze specific chargebacks and disputes when relevant.

Proof-of-Concept process:
Riskified can run either an online pilot where they respond with real-time decisions in the background or offline where order decisions are supplied via csv. It's generally recommended that merchants provide either a target approval rate OR fraud rate in pilots to best gauge performance between competitors on one variable rather than two. Both online and offline pilots require similar integration efforts.

Pricing Format:
Riskified attempts to align incentives to ensure strong ROI. Organizations only pay for approved orders that generate revenue. **Riskified** guarantees approval rates and covers costs of any chargebacks received.

For the guaranteed fraud solution, **Riskified** charges its customers a percentage of every order approved and guaranteed against fraud on behalf of merchants. For other products—Policy Protect and Account Secure—pricing comes as either a monthly platform fee, or per-order (for Policy), or by Monthly Active User (for Account Secure).

Riskified

Integration:

Merchants can integrate with **Riskified** via direct API or by leveraging various prebuilt platform integrations and plugins available through **Riskified's** extensive partner network. Flexible integration paths speed time to go-live and reduce configuration requirements by the merchant. A typical **Riskified** integration can take just a few weeks, including a period of shadow mode (where **Riskified** is receiving live orders but the merchant is not acting upon the decisions). This is intended to calibrate machine learning models and ensure performance from day one.

Riskified can provide synchronous guaranteed decisions in under one second (P99). Pre-authorization optimization recommendations can be provided in under 0.5 seconds (P99), and a typical fraud prevention analysis response time distribution (from certain integration setups) is 600ms, with a median response time of 400ms (P95).

Additionally, **Riskified's** strategy to expand into new geographies includes select "white labeled" partnerships with well-established payment gateway, acquirer, and PSP platforms. For example, there are partners that offer a built-in chargeback guarantee service, powered by **Riskified**. Each of these partner relationships have expertise in specific industry verticals, like gaming, travel, ticketing, and money remittance. Moreover, it also covers different payment methods such as cards, wallets, and direct debit.

Access to integration guides can be found here: https://www.riskified.com/documentation/

Support packages available:

Riskified provides all customers with a complete and comprehensive support structure. Customers do not have to purchase additional levels of support; it is already included in **Riskified's** fees.

ACI Worldwide (ACI Fraud Management)

ACI is a leader in real-time payment solutions, securing the payments ecosystem across commercial banks, central banks, financial intermediaries, merchants, and billers with precision.

ACI occupies a distinctive position within the payments value chain, engaging with customers across various stages. This vantage point provides insights into a vast pool of data. **ACI** empowers its customers and partners by offering access to Payment Intelligence and digital identity services. These services incorporate patented AI models and transactional intelligence.

ACI Payments Intelligence for Banks and Intermediaries

ACI supports financial institutions' ability to identify emerging threats and trends with its predictive modeling capabilities powered by patented incremental learning models. With proven resilience towards fraud risk management and without adding to operational costs, **ACI** is able to deliver data and intelligence from payments across the globe, monitor a transaction and the account relationship, and transform this intelligence into precise and real-time decisioning signals.

For Merchants

ACI Payments Intelligence for Merchants enables a fraud orchestration approach with a customizable, real-time, cloud-based platform using advanced artificial intelligence, machine learning, and behavioral analytics to identify and assess inconsistent and unexpected patterns and behaviors. With the looming threats of synthetic identity, account takeover (ATO), bot attacks/card testing, and the emerging threat of friendly fraud abuse, digital identity is able to verify each transaction's nature in real-time and mitigate threats to reputation and revenue.

ACI Worldwide
Real-Time Payments

At a Glance:

3rd Party API Capabilities | Payment Gateway Capabilities | Operational Support

ACI chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Apruvd

Apruvd is a guaranteed fraud-screening service that combines technology with human involvement to deliver "approve" or "decline" decisions. There are a range of service options, starting with simply backing up an existing program—all the way up to replacing (or serving as an alternative to) in-house teams and platforms. Clients include several Fortune 1000 companies and Internet Retailer Top 500 companies.

Apruvd bases their approach on the idea that ecommerce businesses take on substantial risk to sell products and services online, and managing that risk is difficult and expensive. They attempt to help merchants manage that risk by providing a sustainable, cost-effective solution.

Like most, pricing is based on approvals. If an approval response is returned and it results in a fraud-related chargeback, 100% of the cost is covered. If a decline response is returned, there is no charge.

The service is offered in four customizable tiers:

- **Shop Coverage:** Full application program interface (API) integration where **Apruvd** will screen 100 percent of sales, guaranteeing all associated fraud-coded chargebacks.
- **International coverage:** Similar to the above, with a focus on selling to any country in the world.
- **Select Orders:** Choose certain orders to protect against fraud, using a manual selection process or a rules-based system.
- **Declines Only:** Recover lost sales, and connect with more customers by letting **Apruvd** cover your risk. Before declining any order, submit it to **Apruvd** for a second opinion. If they approve it, merchants have zero risk. If they decline it, nothing is owed.

Integration through the direct portal ("select orders" and "declines only") can take place in under 10 minutes. Average turnaround times for full API integration are less than one day.

At a Glance:

Apruvd chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Arkose Labs

Arkose Labs enables businesses to manage fraud and abuse at scale by combining sophisticated risk-based decisioning with intelligent authentication challenges.

Its unified platform undermines the economic drivers behind organized fraud by introducing targeted friction to risky traffic. This can block automated attacks and occupy resources needed to execute human-driven attacks, rendering large-scale attacks financially non-viable.

Its dual approach encompasses **Arkose Detect**, the risk decision engine, with **Arkose Enforce**, a challenge-response mechanism. While trusted users largely proceed unchallenged, traffic from bots, sweatshops and fraudsters is classified according to its risk profile and presented with custom step-up challenges. Visual enforcement challenges are simple for true users to solve, but prevent fraudsters from circumventing them at scale. Authentication puzzles are constantly evolving to stay ahead of fraudsters and cannot be solved by machines.

Solution highlights include:

- **Unified platform:** Combined risk-based and step-up authentication
- **Deep analytics:** Deep device and network forensics to detect the most subtle signs of fraud
- **Enforcement challenges:** Targeted challenges which adapt to the risk classification of traffic
- **Embedded machine learning:** Self-optimizing platform which improves with each transaction
- **100% SLA guarantee:** The only vendor to guarantee protection against large-scale attacks

Arkose Labs

At a Glance:

Fraud Engine/ Platform Functionality

Guaranteed Chargeback Liability

Arkose Labs chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

ClearSale

ClearSale provides a complete, data-science-backed fraud solution that supports prevention of chargebacks and false declines to optimize the shopping experience.

Ecommerce fraud and chargebacks can quickly chip away at a merchant's bottom line, but false declines can turn legitimate customers away. This is why **ClearSale** focuses on both chargebacks and false declines. **ClearSale** combines sophisticated AI technology and a proprietary secondary review process to help maximize a business's revenue, approve as many valid orders as possible, and keep customers happy.

False Declines Cost More Than Fraud

Rather than looking for reasons to decline orders, **ClearSale** focuses on reasons to approve them. Occasionally, good orders can look like fraud, and chances are, those orders are getting declined and putting good customers off.

While most ecommerce merchants focus on managing fraud and chargeback costs, the cost of revenue lost to false declines (also known as false positives) is far more expensive.

ClearSale never auto-declines orders. Every order is reviewed systematically. ClearSale's proprietary A.I. technology "learns" each unique business model and builds a custom fraud-scoring algorithm that matches the fraud risk profile of the business.

Any incoming order that is scanned and found to be potential fraud is sent for an advanced secondary review where the transaction is dissected to validate whether the order is truly fraudulent.

ClearSale

At a Glance:

Arkose Labs chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

DataVisor

DataVisor is a fraud and risk management platform powered by AI technology. Combining an extensive set of tools and machine learning approaches, the platform enables a holistic fraud prevention strategy that includes Supervised and Unsupervised learning techniques, rules engine, automated feature engineering, native device intelligence and visual link analysis, **DataVisor** delivers complete control to enterprises looking to manage against fraud without sacrificing customer experience.

DataVisor protects global clients across digital commerce, fintech, marketplaces, travel platforms, and financial services against financial loss. **DataVisor** supports complete account lifecycle protection starting with account opening fraud, payment and chargeback fraud, ATO, promotion and policy abuse, application fraud, transaction fraud, AML and more. Verticals of focus include financial institutions, fintech, travel, insurance, digital commerce, marketplace and gaming.

KPIs of focus include: fraud rate, false positive rate, time to detect new fraud, manual review rate, auto accept/reject rate, and review efficiency rate.

DATAVISOR

At a Glance:

3rd Party API Capabilities

Device Intelligence Capabilities

Fraud Engine/ Platform Functionality

ThreatMetrix chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Feedzai

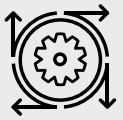
Feedzai attempts to provide a machine-learning-based fraud platform to help risk professionals do the work of data scientists using a guided, self-contained environment. Through **Feedzai DS**, teams are provided with a way to create advanced machine-learning fraud models. With extraction of features, feature engineering, model generation, and evaluation, **Feedzai's** application interface guides users through the development of risk-based algorithms.

Feedzai attempts to increase accuracy by profiling every data point and moving away from loose-fitting segmentation. They do this by treating each customer, device, Internet Protocol (IP), etc. as a **Segment of One**, and not a sample of many.

With a focus on omni-channel commerce, **Feedzai** looks to work through a variety of user interfaces, including:

- Ecommerce, in-store
- Mobile, desktop, tablet devices
- ATM, in-branch
- Mail Order/Telephone Order (MOTO), petrol/Automated Fuel Dispenser (AFD)

At a Glance:



AI Powered

Fraud Engine/ Platform Functionality

Feedzai chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Identiq

Identiq is a private network that supports companies in making better risk-based decisions by utilizing the collective trust and knowledge companies have on customer identity in a completely private way. The peer-to-peer network allows companies to safely collaborate with each other to validate trusted customers without sharing any sensitive data or identifiable information. The cryptographic technology allows network members to ensure that the physical and digital attributes of users match those of the other members.

The organization was launched in 2018 and provides insights on more than three billion identities in over 160 countries. The technology generates a trust score based on the consensus of the network, helping businesses understand who is a good customer to offer frictionless experiences to, and who is fraudulent and should be blocked. **Identiq** addresses problems with third-party and obsolete data by having fresh and untapped first-party data from some of the world's largest companies. This is possible because, with a patented protocol, no personal data ever leaves the members' environment. PII is never shared, not even with Identiq.

Each network member installs an "edge server" on-site. This is the cryptographic protocol based on secure multiparty computation, and includes a normalized database that remains in the member's environment at all times. Each member joins with all their data in order to participate in the validation of users against other members' databases. When a company queries the network, they send a one-time fully anonymous query to the other members to ask if they already know and trust the customer. Based on the responses and degree of confidence, **Identiq** provides a score with sub-second response time.

Industries of focus include ecommerce, fintech, travel, ticketing, and marketplaces.

IDENTIQ

At a Glance:

3rd Party API Capabilities

Historical Sandbox Testing

AI Powered

Identiq chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Kount, An Equifax Company

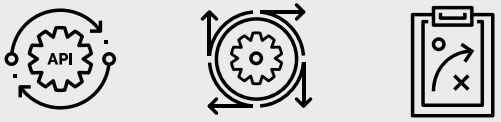
Kount was acquired by **Equifax** in early 2021. Midigator, a chargeback technology company, was also acquired in 2022 and merged into the same organization with Kount, which resulted in the formation of the Digital Solutions team at Equifax. Combined, Equifax, Kount, and Midigator power digital risk assessment, helping businesses establish greater identity trust behind each consumer interaction. With **Kount, Equifax** expands the company's worldwide footprint in digital identity and fraud prevention solutions. Global businesses can harness the power of AI better than ever before to establish strong digital identity trust—and engage better with their customers online. With **Midigator**, businesses have complete protection across the entire customer journey—from checkout to chargeback response.

Kount's Digital Identity Global Network delivers real-time fraud prevention and account protection. It enables customer experiences for more than 20,000 brands and works with over 70 payment processors and card networks. Linked by **Kount's** award-winning AI, the Digital Identity Global Network analyzes signals from 56 billion annual interactions to personalize user experiences across the spectrum of trust—from frictionless experiences to fraud blocking. Their Identity trust decisions focus on delivering safe payments, account creation, and login events while reducing digital fraud, chargebacks, false positives, and manual reviews.

Kount's artificial intelligence, combined with the Digital Identity Global Network, empowers businesses to establish trust or risk in real time throughout the customer journey. **Kount's** AI combines both supervised and unsupervised machine learning to analyze billions of fraud and trust-related identity signals and to deliver identity trust decisions.

Kount® An Equifax Company

At a Glance:



3rd Party API Capabilities

AI Powered

Operational Support

Kount chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Kount, An Equifax Company

For each transaction, Kount's AI produces an identity trust Omniscore, an actionable fraud score that simulates the judgment of an experienced fraud analyst. Businesses use these predictive scores to reduce manual reviews and a reliance on policies that react to fraud only seen in past instances.

NoFraud

NoFraud is a full-service fraud prevention solution offering automated ecommerce fraud prevention through real-time virtual identity verification. They deliver individual, real-time decisions for each transaction using thousands of data points and virtually

Pre-gateway Integration: **NoFraud** is able to screen and decline a transaction before the customer checks out, prompting customers to re-input their information. This lowers the number of declines occurring due to typos or missing or incorrect information. This integration route allows **NoFraud** to view the card attempts, providing **NoFraud** with additional cardholder behavior data. This integration also allows **NoFraud** to stop card testing attacks, which prevents those transactions from reaching the payment gateway and reduces the impact of bot attacks.

Cardholder Verification: **NoFraud's** Cardholder Verification process allows **NoFraud** to validate high-risk transactions by reaching out to the cardholder for verification. This process is customizable based on a client's specifications.

Integrations: A client can integrate via shopping cart app, API, or gateway emulator. Apps are available for several shopping platforms, including Shopify, Magento, BigCommerce, and WooCommerce. API integration allows for compatibility with any platform. A gateway emulator is also available for most popular payment gateways.

Chargeback Protection: **NoFraud** offers a chargeback guarantee and will reimburse the customer for fraud chargebacks that occured on transactions it accepted.

NOFRAUD

At a Glance:

Fraud Engine/ Platform Functionality

Guaranteed Chargeback Liability

AI Powered

NoFraud chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

NOTO

NOTO takes the approach that seemingly different use cases such as fraud prevention, AML, account compromise, and credit risk have common roots in the underlying event data. **NOTO** can process data in a range of ways and deliver ample and instant decisions. A single integration is all it takes to enable companies to consolidate their approach to fraud and risk management.

NOTO is built by financial crime prevention specialists, for specialists in the field. The solution has been developed so that it helps solve for the biggest industry challenges, and to address KPIs specifically related to:

- Reduction in manual reviews
- Adherence to card scheme metrics
- Reduction of false positives
- Improvement of acceptance and customer friction reduction

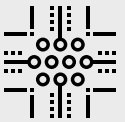
Solutions and Functionality

While businesses are concerned about cybercrimes, they often don't know how best to prevent them and where to start. **NOTO** believes that to get a comprehensive view of the threat landscape, quickly identify suspicious activities, and streamline investigations, companies need to better coordinate their anti-fraud and AML controls.

NOTO

YOUR DATA. YOUR WAY. NO LIMITS.

At a Glance:



Non-Production
Real Time Rules Testing

Fraud Engine/
Platform Functionality

Professional
Guidance/Services

Arkose Labs chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Outseer

Outseer, an RSA company, provides payment authentication, account monitoring and fraud management technology solutions to support secure growth of digital commerce. **Outseer** products and solutions have been built using identity-based science and machine learning to deliver high detection rates with little to no customer intervention, allowing for a more seamless user experience. **Outseer** processes more than 20 billion transactions globally, protecting more than two billion consumers each year.

Products, Solutions and Technologies:

- **Outseer** 3-D Secure™ is a risk-based, card-not-present (CNP) and digital payment authentication solution mapping to the latest EMV® 3-D Secure protocol. For more information regarding the **Outseer** 3-D Secure solution, see pages 35-37
- **Outseer** Emerging Payments™: **Outseer** Emerging Payments provides continuous authentication solutions for new types of digital commerce transactions. Buy Now, Pay Later (BNPL) Installments is the first payments solution being offered within the new Outseer Emerging Payments platform. Two key differentiating aspects of Outseer products and solutions are the Outseer Risk Engine™ and the **Outseer** Global Data Network™:

OUTSEER
An RSA Company

At a Glance:

Outseer chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Ravelin

Ravelin works with ecommerce retailers, online marketplaces, fintechs, and financial institutions by request. They operate in 185 countries, producing over six billion fraud scores annually (through both direct and indirect integrations). They help predict risk with accuracy and speed to allow clients to reduce fraud and accept more secure payments. Verticals of specialization include: travel, transportation (on-demand taxi apps), event ticketing, transport ticketing, retail (grocery, fashion, electronics, Fast Moving Consumer Goods (FMCG)), gaming and online marketplaces.

The **Ravelin** Rules Engine gives users the ability to create and test rules at any time. Rules operate on the full set of underlying data elements and inputs that they support, and can be used to create specific outcomes on customers and orders, or apply tags and labels which can feed into review or triage processes.

Clients have full control over their rules, although their approach to fraud prevention often recommends rules are used for "business policy" decisions, and that fraud detection recommendations are powered by machine learning. **Ravelin's** core payment solution can be extended easily to include a number of different use cases that are emerging as key threats to ecommerce. They require small additional pieces of data that are documented in the API. The recommendations can be inserted into the customer purchase flow where appropriate.

All can be viewed and reported on within the **Ravelin** dashboard. All clients take advantage of **Ravelin's** unique graph database, which analyzes and visualizes connections in data and uses advanced techniques to provide actionable insights from those connections.

Ravelin

At a Glance:

Ravelin chose not to participate in the Paladin Vendor Report at this time.
If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Sardine

Sardine offers a unified platform for fraud prevention, AML compliance, and payment risk management. It primarily serves banks, fintechs, and online retailers, helping them manage account creation fraud, identity and business verification, payment fraud, AML monitoring, and chargeback handling. With a history in the financial services and cryptocurrency sectors, the company has extensive experience managing extreme risk.

Handling 960 million transactions per year totaling over $150 billion, their volume is growing by 5-10% every month. They support clients' goals by focusing on fraud loss rates, fraud prevention program operating expenses, approval rates, account takeovers, suspicious AML activity count, and payment fraud rates (such as chargeback and unauthorized return rates). Last year, the company prevented more than $21.3 billion in potential fraud losses.

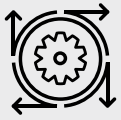
Solutions and functionality:

The **Sardine** platform includes multiple tools for managing fraud and AML compliance. It includes a comprehensive dashboard for user, session, and transaction investigation. The platform can analyze program performance and write business logic for specialized use cases. **Sardine** facilitates fraud management for various payment methods, Know Your Customer / Know Your Business (KYC/KYB) compliance, document verification, AML transaction monitoring, case management, and data enrichment (such as identity, open banking, blockchain, and email/phone data). It also handles machine learningbased risk scoring and includes various investigative tools like customer intelligence, device intelligence, network graph, and anomaly detection.

sardine

At a Glance:

3rd Party API Capabilities



AI Powered

Guaranteed Chargeback Liability

Sardine chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

SEON

SEON helps organizations identify fake accounts, reduce manual reviews, and better manage chargebacks. The Intelligence Tool modules integrate via REST API, and non-developers can even leverage the Admin Panel or the innovative Chrome extension to manually enrich data in one click.

Social media lookup:
Perform background checks with data points from 20+ social media platforms.

Precise risk scores:
Get accurate risk scores for more informed business decisions. Manually adjust the thresholds that automatically block suspicious users and manage false positive rates as you see fit.

Compliant and fast:
SEON aggregates info in near real-time from live, open-source databases. Connections are anonymous and SSL-protected, and no logs or sensitive info are stored for data protection compliance.

At a Glance:

SEON chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Signifyd

Signifyd's Commerce Protection Platform helps address fraud challenges at key conversion points across the ecommerce shopper journey, from account creation to return request. By eliminating fraud and abuse throughout the funnel, the platform allows merchants to protect revenue, trust customers, and promote growth. **Signifyd** supports a large number of enterprise customers, including two of the world's top three online retailers. **Signifyd** is headquartered in San Jose, California, with locations in Denver, New York, Mexico City, São Paulo, Belfast, and London.

Signifyd helps merchants:

- **Protect Revenue:** In addition to addressing fraud itself, the platform helps to address fear of fraud, which can create barriers to conversion. These barriers can include login step-ups, authorization declines by issuing banks, declines within the fraud management process, the potential for stockouts that can result from manual review delays, and the lost revenue due to chargeback fraud and return abuse. **Signifyd** helps merchants assess these conversion points – identifying opportunities to reduce friction across the funnel and implementing enhancements to streamline the path to purchase for good customers.
- **Trust customers:** To compete on customer experience requires a fast and secure checkout, avoidance of authentication step-ups, and quick order fulfillment. With a high shopper identification rate, **Signifyd** supports increased trust that can help to deliver these shopping experiences.
- **Grow Fearlessly:** Chargeback liability often leads to decisions made by fear of loss. By shifting liability away from ecommerce merchants, **Signifyd** helps eliminate the roadblock of fear to enable fearless growth. The platform allows merchants to more confidently launch new products, expand internationally, offer omnichannel shopping experiences, and establish flexible business policies and customer rewards.

Signifyd

At a Glance:

3rd Party API Capabilities | Operational Support | AI Powered

Signifyd chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Sift

The **Sift** Digital Trust & Safety Suite, powered by real-time machine learning, assesses risk of billions of live events taking place on desktop and mobile applications across its global network of customers. With over 34,000 sites and apps represented across the platform, **Sift** customers benefit as the solution collects, analyzes, and learns from millions of legitimate and suspicious events every minute.

Based on these events, **Sift** assesses the risk of account creations, logins, orders, user-generated content, and unique events so merchants can make instant and accurate decisions, automate, and scale fraud operations. By taking a holistic look at the user journey, **Sift** is able to detect multiple types of fraud (payment fraud, spam, scam content, phishing attempts, account takeovers, promotion abuse, and fake accounts) and provide a risk assessment of each interaction.

The **Sift** global model anonymously shares insights about new, emerging fraud patterns across the network, boosting prediction accuracy. **Sift** combines global models with custom learning and extensive feature engineering to deliver accuracy and enable dynamic, real-time decisioning. These blended global and custom models adapt to the specific use cases of a business, in order to uncover and track fraud patterns that are unique to them. **Sift** also performs extensive feature engineering on individual data elements to generate tens of thousands of signals across identity, device, behavioral, and transaction vectors.

Sift's products offer organizations with the flexibility to serve as either the primary fraud tool, or as a key input of a larger, layered approach. Customers can access their data and results by ingesting it via APIs or using **Sift's** customizable web-based Console.

At a Glance:

3rd Party API Capabilities

AI Powered

Fraud Engine/ Platform Functionality

Sift chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Vesta

Vesta is a transaction guarantee platform focusing on digital purchases. They support organizations in the pursuit to eliminate all the costs associated with fraud. This includes direct losses as well as lost sales and unnecessary declines.

The solution utilizes machine learning to increase approvals of legitimate sales while eliminating chargebacks and other forms of digital fraud. **Vesta** maintains teams around the world working in a number of regions including North America, Latin America, Europe, and Asia-Pacific.

Founded in 1995, **Vesta** provides revenue-generating payment solutions to enterprise partners who support online ecommerce and card-not-present transactions. Industries include ecommerce Retail, Telco, Travel & Hospitality, Financial Services, Payment Service Providers (PSPs)

The solution helps organizations focus on a range of KPIs including:

- Reducing the number of fraudulent chargebacks
- Reducing or eliminating costs from chargebacks
- Increasing the number of legitimate orders
- Increasing revenue from approval of more legitimate orders

Solutions and functionality:

Vesta Payment Guarantee is full-service fraud protection that guarantees decisions in real time for every transaction. Payment Guarantee clears the path for legitimate customers to purchase more easily, while simultaneously blocking malicious transactions from fraudsters, resulting in risk-free revenue.

At a Glance:

Guaranteed Chargeback Liability

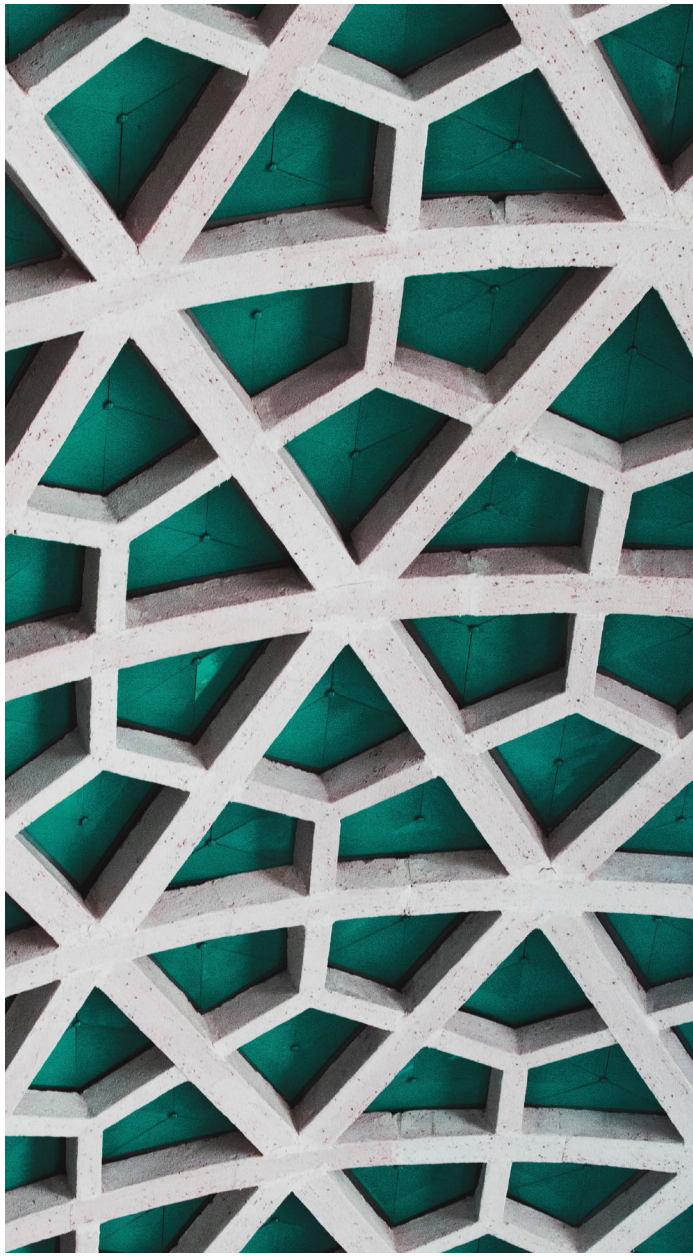
AI Powered

Fraud Engine/ Platform Functionality

Vesta chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Identification & Data Verification

By linking people, places, and things, these services can help increase trust through a clear understanding of the person behind every transaction or interaction. Moreover, these services can go a long way in determining whether the data is directly associated with the cardholder or a friend or family member of the cardholder. These services are especially useful in cases where the user or customer is required to provide personal identity data or physical ID.



Socure

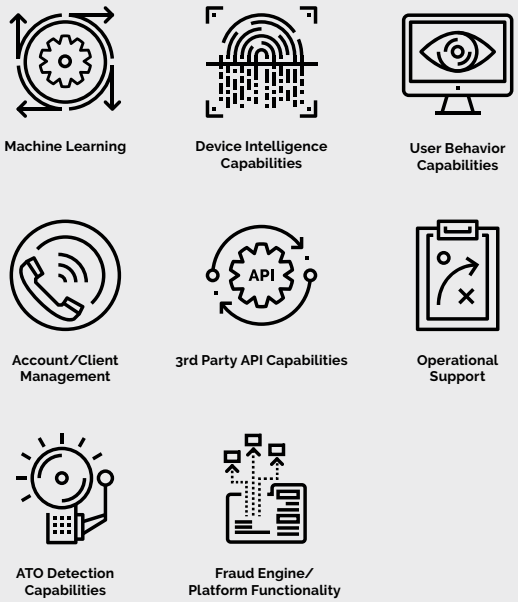
Socure is a leading provider of AI-powered digital identity verification and fraud prevention solutions, trusted by some of the largest enterprises and government agencies to build trust and mitigate risk, anytime through the customer lifecycle. Extensively leveraging AI and machine learning, **Socure's** platform helps users achieve some of the highest accuracy, automation and capture rates in the world. With the acquisition of Effectiv in 2025, **Socure** expanded its capabilities to offer end-to-end identity fraud and payment risk management, integrating advanced transaction monitoring, credit underwriting and know-your-business (KYB) solutions into its platform.

Socure delivers a single, unified platform for identity trust—from stopping identity fraud andmaximizing good customer acceptance at onboarding, to verifying businesses with precision, preventing unauthorized transactions, and optimizing risk-based decisioning, **Socure** uses AI to address emerging threats and restore digital trust.

CEO Johnny Ayers founded **Socure** in 2012, with a mission to verify 100% of good identities in real time and completely eliminate identity fraud.

Banks, fintechs, public agencies, marketplaces, gaming, workplaces, and many other verticals rely on **Socure** to deflect attack and scale safely. Socure serves 3,000+ customers, including 18 of the top 20 U.S. banks, 13 of the top 15 credit card issuers, 6 of the top 7 sportsbooks, 600 leading fintechs, the top 2 gig platforms, 4 of the top 5 social media platforms, the top 4 HR information systems, and 132 public organizations, delivering secure, accurate digital identity infrastructure at scale worldwide.

At a Glance:



Platform Highlights

Unified Identity, Fraud, Compliance, and Risk Decisioning

RiskOS® is **Socure's** unified platform for identity verification, fraud prevention, compliance, and risk decisioning. It consolidates what has historically required multiple vendors and disconnected point solutions into a single platform and API, enabling organizations to make precise, real-time decisions across the entire customer lifecycle, from onboarding and authentication to transactions, account changes, and recovery.

For community financial institutions managing identity, fraud, and compliance with limited technical staff, **RiskOS** can eliminate the operational requirements of integrating and maintaining separate systems for KYC, KYB, AML screening, account takeover prevention, and payment screening. The platform provides a no-code strategy builder that allows risk and compliance teams to configure, test, and deploy decisioning workflows without engineering resources. Pre-built workflow templates developed by industry veterans address common use cases out of the box, and the platform's drag-and-drop canvas enables teams to design and deploy complex decision logic with complete audit history, adapting to new threat vectors in real time without waiting on IT.

RiskOS integrates **Socure's** own AI-powered identity and fraud intelligence with a broad ecosystem of 180+ pre-integrated third-party data services, all accessible through a single API connection. This means institutions gain access to extensive data coverage without procuring, integrating, or managing individual vendor relationships.

Identity Graph and SocureID

Every decision in **RiskOS** is powered by **Socure's** proprietary Identity Graph, the largest in the industry, comprising hundreds of billions of identity elements and 40 billion historical known outcomes. This consortium-driven data asset creates a compounding network effect: the more organizations that contribute outcomes, the more accurate and comprehensive the intelligence becomes for every participant.

Socure's Identity Graph achieves a 96.4% identity recurrence rate, meaning the vast majority of identities presented to the platform have already been seen and verified within the network. With 314 million recurring identities, the platform provides a holistic risk view that includes verified devices, email addresses, phone numbers, transaction history, and behavioral analytics.

SocureID: A Persistent Identity Anchor Across Use Cases.

Each identity that passes through RiskOS is resolved and mapped to a unique **SocureID**, a single persistent identifier that connects every email, phone number, address, device, behavior, KYC result, and watchlist decision into one unified profile within

Socure

Socure's Identity Graph. **SocureID** removes duplicates, preserves historical context, and ensures that every decision made about an identity, whether at onboarding, login, payment screening, or account recovery, draws from the same resolved source of truth. For community financial institutions, **SocureID** eliminates the fragmentation that occurs when different systems maintain disconnected views of the same customer, creating a single thread of identity intelligence that spans the entire member or customer relationship.

Proactive Risk Notifications. Because **SocureID** maintains a persistent, continuously updated profile for each resolved identity, RiskOS enables organizations to receive proactive alerts when the risk profile of an individual changes over time. Rather than relying solely on point-in-time checks at onboarding or login, institutions are automatically notified when identity attributes shift, new fraud signals emerge, sanctions or watchlist exposure changes, or consortium-level risk patterns are detected. This shifts risk management from a reactive posture, where threats are only caught when a customer initiates an action, to a proactive model where the institution is alerted to emerging risks before they result in losses. For community financial institutions with limited fraud investigation staff, proactive notifications ensure that high-priority risks surface automatically rather than depending on manual portfolio reviews or periodic batch screening.

Multi-Tiered Graph Intelligence: Local and Global

Socure's graph strategy operates at two tiers, each delivering distinct value:

Global Graph. The Global Graph is **Socure's** cross-industry consortium intelligence layer, built on hundreds of billions of identity elements and 40 billion known outcomes from 3,000+ customers. It powers **Socure's** AI models and risk scores by providing cross-institution visibility into fraud rings, velocity anomalies, synthetic identity patterns, and first-party fraud behavior. Community financial institutions benefit from the same consortium intelligence that protects 18 of the top 20 U.S. banks and over 600 fintechs. Fraud patterns identified at the largest institutions immediately strengthen protections for every customer on the platform, without smaller institutions needing to build or maintain proprietary data assets of their own.

Local Graph. Local Graph is an enterprise-specific intelligence layer within **RiskOS** that connects every identity to its activities and risk signals across an organization's own ecosystem in a single, time-aware framework. Where the Global Graph provides cross-industry intelligence, Local Graph gives fraud, risk, and trust teams the ability to see how an identity appears today, how it has behaved historically within their institution, and how individual identity elements such as devices, phone numbers, emails, and IP addresses relate to one

another over time. Local Graph is supported by two capabilities:

1. **Persistent Profiles** provide a dynamic, always-on view of how any identity element interacts with an organization over time. Profiles unify every known interaction, signal, and linkage, eliminating blind spots and giving analysts a complete understanding of historical context in a single place.
2. **Connected Rule Writing** allows organizations to build decisioning rules using historical activity, relationships, and velocity patterns rather than relying solely on point-in-time data. Teams can incorporate behavior from earlier touchpoints, including account opening, password resets, logins, transactions, and disputes, into automated decisions.

Together, the Global Graph and Local Graph give community financial institutions two layers of fraud intelligence that would be impossible to replicate independently: the collective knowledge of the industry's largest consortium, combined with institution-specific behavioral patterns that surface risks unique to their own portfolio and member base.

AI-Native Platform with Embedded Intelligence

RiskOS embeds AI throughout the platform, not as an add-on feature but as core infrastructure. The **RiskOS** AI Suite, launched in late 2025, includes six purpose-built AI agents and assistants that automate and accelerate key tasks across the risk lifecycle. A rule writing assistant enables compliance and fraud teams to create executable decisioning rules in plain language through a no-code interface. A case review assistant suggests case outcomes based on scores, signals, and user history, reducing manual review time and improving consistency. A business intelligence agent automates KYB due diligence by scanning a company's full public web presence, ownership structure, and adverse mentions, cutting 30+ minutes per review. GenAI-powered explainability provides one-click, plain-language explanations of model scores and workflow decisions, strengthening audit trails and supporting regulatory transparency.

These capabilities directly address a persistent challenge for community institutions: maintaining effective fraud and compliance operations with small teams. By automating rule creation, case triage, and decision documentation, RiskOS reduces the specialist headcount required to operate a sophisticated risk program.

Primary Use Cases for Community Financial Institutions

RiskOS supports end-to-end fraud, risk, and compliance operations through pre-built, configurable use cases designed for the needs of community banks and credit unions:

Consumer Onboarding. Integrates identity verification, fraud risk scoring, KYC, and compliance screening into a single workflow. As a leading platform, it achieves approximately 90% automated approval rate while minimizing fraud and friction. Advanced Pre-Fill capability

verifies identities with just two pieces of PII and an authentication method, reducing application abandonment and accelerating time to account opening.

Business Onboarding (KYB). Automates Know Your Business verification, Ultimate Beneficial Owner (UBO) checks, and entity risk assessment. Platform integrations with partners like Middesk and Markaaz deliver comprehensive business intelligence, cutting 30+ minutes per manual review and reducing the operational burden of commercial account onboarding.

Login and Account Takeover Prevention. Provides real-time authentication and risk-based step-up verification triggered by device, behavioral, and identity signals. The platform detects and blocks unauthorized access attempts, including those driven by GenAI-powered spoofing of emails, phone numbers, and geolocations, while minimizing friction for legitimate users during login, password resets, and account recovery.

Bank Account Verification. Validates account ownership and status in real time, supporting secure account funding, direct deposits, loan payments, and transfers. The solution proactively prevents unauthorized transactions and reduces fraud risk in money movement. Coverage has recently expanded to 30+ countries for institutions with cross-border needs.

Workforce Verification. Confirms that job applicants are real, legitimate individuals at the start of the hiring process by validating identity, device, and behavioral signals against authoritative data. Blocks over 70% of fraudulent applicants before they reach recruiters. For employees, it extends verification into ongoing access to systems, data, and payroll through persistent identity checks, sanctions and watchlist screening, and risk-based step-up verification. **SocureID** ties applicant screening and ongoing employee checks to the same resolved identity, ensuring consistent and auditable risk evaluations from hiring through access and payroll.

Payment Screening. Provides sanctions screening and watchlist monitoring to support BSA/AML compliance obligations. Socure's Global Watchlist Screening with Monitoring uses an AI-driven, two-stage matching approach that improves match precision and lowers false positives compared to legacy solutions, reducing manual review effort and strengthening auditability.

Socure's Product Highlights

Sigma Identity Fraud is **Socure's** market-leading solution for detecting and preventing third-party identity fraud at onboarding and across the customer lifecycle, delivering a holistic, AI-driven approach by analyzing every identity element in real time.

It uniquely combines personally identifiable information (name, email, phone, address, date of birth, SSN) with digital signals

including device intelligence, behavioral analytics, IP address, geolocation, relationship data, and historical transactional patterns from **Socure's** Identity Graph, powered by billions of outcomes from 3,000+ customers across 20+ markets. By assessing these patterns across institutions, geographies, and timeframes, Sigma Identity Fraud detects anomalies that signal identity theft or manipulation at the entity level, achieving up to 89% fraud capture in the riskiest 5% of applicants and up to 85% in the riskiest 3%—more than double the industry average—while reducing false positives by over 40% and driving manual review rates below 5%.

Sigma Synthetic Fraud is Socure's market-leading solution for detecting and preventing synthetic identity fraud in real time. Purpose-built to address its unique and evolving nuances, this AI-driven model leverages synthetic-specific features to identify even the most sophisticated fabricated and manipulated identities in real time.

The result is best-in-market performance, capturing up to 83% of synthetic fraud within the riskiest 5% of applicants, enabling institutions to stop synthetic identities at the door while preserving seamless approval experiences for legitimate users, including hard-to-verify and thin-file populations.

Sigma First-Party Fraud is a consortium-based solution that stops bad actors at scale by providing visibility into their activity across the broader financial ecosystem. As the largest cross-industry first-party fraud consortium, it brings together a uniquely diverse network of organizations across financial services, fintech, online gaming, BNPLs, payment apps, credit unions, marketplaces, and more. In 2025 the consortium achieved significant scale, amassing data intelligence encompassing 416+ million identities, 20+ billion transactions, and 520+ million accounts.

Sigma First-Party Fraud is the only holistic first-party fraud solution that delivers two predictive risk scores — Identity Manipulation Score and Dispute Abuse Score — as well as real-time, actionable intelligence to help detect repeat abusers and predict the risk that a true identity will act in bad faith. This proactive approach helps organizations drastically reduce losses, cut operational costs, and build a trusted ecosystem for good users.

Backed by the largest cross-industry consortium, Sigma First-Party Fraud analyzes risk signals — such as dispute patterns, payment denials, and account closures — to uncover individuals who manipulate their identities or financial behavior for bad-faith activities. These real-time insights, combined with the two aforementioned risk scores, quantify the likelihood of an individual engaging in first-party fraud after account opening. Additionally, real-time alerts enable organizations to take immediate action, preventing repeat fraud and minimizing risk exposure.

Socure

Email, Phone, and Address RiskScores verify the trustworthiness and ownership of a phone, email, or address to enhance fraud and scam detection across the customer lifecycle. These machine-learning models evaluate newly presented PII to distinguish legitimate users from sophisticated threats with minimal user input.

Email RiskScore assesses the risk of a name/email pair in real time by verifying the correlation of these elements and evaluating hundreds of good-versus-risky signals, including indicators of fake, machine-generated, invalid, high-velocity, and low-tenure email usage associated with that identity. It performs real-time anomaly detection at the individual, company, industry, and network level to uncover unusual identity–PII linkages and risky behavior patterns, while leveraging consortium and authoritative data to distinguish trustworthy from suspicious associations. Additionally, Email RiskScore measures how often an email has been linked to an identity, as well as the frequency of risky or trustworthy outcomes tied to that pairing, to drive more accurate decisions.

Phone RiskScore confirms name/phone ownership and assesses the risk associated with phone numbers to enable proactive fraud prevention with enhanced confidence and accuracy. The solution analyzes phone-specific intelligence such as line type and tenure, carrier information, and identity–PII velocity, and checks against Socure's proprietary positive and negative phone data and broader network identity graph. It also performs real-time anomaly detection and SIM swap detection to flag high-risk changes or usage patterns that could signal account takeover or other forms of fraud.

Address RiskScore helps prevent malicious actors from hijacking or creating accounts with compromised or synthetic physical addresses by verifying the validity of a given address and determining the strength of association between the address and the identity. The solution analyzes a wide range of address-related signals such as delivery and mail activity patterns and the characteristics of P.O. boxes, commercial locations, military addresses, correctional facilities, and more, enabling incredibly broad and accurate address verification.

Digital Intelligence Suite delivers real-time, actionable risk and trust signals across the entire digital journey—from onboarding and login to high-risk transactions and contact center flows.

Bringing together three core services in real-time in 200ms — Device Intelligence (device-level across 900M device signals per month and network risk signals), Behavioral Analytics (session-based behavior analysis), and Entity Profiler (PII-to-device linkage and digital presence)—the suite binds each identity to its devices, behaviors, and historical interactions to continuously detect anomalies and prevent account takeover and abuse.

Powered by hundreds of device, behavioral, and network signals, Digital Intelligence forms a single, comprehensive risk layer that

feeds directly into Socure's AI models listed above—such as Sigma Identity Fraud, Sigma Synthetic, First-Party Fraud, and Predictive

DocV—and is fully orchestrated through the RiskOS decisioning platform. This enables a true, comprehensive view of identity—going beyond confirming a customer is who they claim to be to also determine whether they are a real person and whether it's safe to do business with them. Persistent identity decisioning provides a dynamic "digital signature" for each user, giving organizations a unified, cross-session view of risk.

Socure's Compliance Suite provides seamless, automated compliance across the entire customer journey. It's delivered via a single API and unifies customer verification, sanctions screening, ongoing monitoring, and decisioning into one orchestrated Workflow—offering extensive data coverage, precision, accuracy, and controls that can help stand up to regulatory scrutiny.

Socure Verify delivers accuracy, reasoning, address verification, and risk alignment for Customer Identification Program (CIP) and KYC verification. Powered by AI and machine learning, Socure's triangulated data approach can help verify identities across multiple trusted sources to support CIP and KYC requirements, correlating thousands of online and offline identity signals to resolve to the single best matched entity. This methodology enhances fraud detection, reduces false positives, and can support compliance while enabling seamless onboarding for all demographics, including hard to identify populations.

Socure achieves verification rates of up to 99% for mainstream populations and industry-leading, high-90s verification rates for Gen Z and other thin-file or new-to-country applicants. With considerable Gen Z coverage, **Socure** verifies 70% of 18-year-olds opening their first financial accounts—30% more than legacy providers—and delivers verification rates in the mid-90s for 18- to 25-year-olds. Additionally, **Socure** delivers high verification rates for 13- to 17-year-olds. Available in over 190 countries, **Socure's** proprietary models and verification techniques, can support precise identity matching even in cases of name variations, nicknames, misspellings, or reordered name structures.

Electronic Consent-Based Social Security Number Verification (eCBSV) provides an additional identity verification layer to combat synthetic identity fraud and enhance CIP compliance. By directly matching an individual's name, Social Security Number (SSN), and date of birth (DOB) with the issuing authority, eCBSV enables businesses to make confident decisions, especially for higher-risk consumers, while delivering a 6–8% average additional approval lift for hard-to-identify, thin-file populations such as Gen Z, new-to-country, and other underserved consumers. By using this service, businesses can strengthen fraud prevention, enhance regulatory compliance, and expand access to previously hard-to-verify

Socure

individuals, ensuring more accurate and efficient identity verification.

Socure's Global Watchlist Screening with Monitoring enhances compliance operations with advanced AI and ML, delivering sanctions matching accuracy and scale. A two-stage scoring system—combining name matching with advanced entity resolution and profile matching—helps provide certainty that the individual in question is the correct match, while minimizing false negatives and unnecessary alerts.

By integrating intelligent risk assessment, continuous status monitoring, and streamlined case management, **Socure's** solution is 20% more accurate than competing approaches, reduces false positives by 30%, and drives a 75% reduction in manual reviews. Analysts gain a single, workspace to view side-by-side comparisons, prioritize critical cases, and capture reviewable context for audits, supported by daily sanctions, PEP, and adverse media updates. With tiers of global coverage and configurable match parameters, Socure empowers teams to maintain compliance, reduce operational burden, and focus on truly high-risk entities.

Socure's Predictive DocV (DocV) solution verifies a consumer's government-issued identity document against their facial biometrics using advanced document forensics and machine learning–driven decisioning. It is built to handle high volumes of stolen identities, spoofing, and highly sophisticated deepfake and injection attacks that are increasing in complexity.

Socure's proprietary solution addresses multiple attack vectors using a layered approach to protect against fraud, with no impact on the user experience. This strategy analyzes a rich set of document signals in real time, with a broader view of identity risk by also analyzing PII, barcode data, device and behavioral intelligence, geolocation, and biometric signals. Advanced deepfake and injection detection models can analyze camera integrity, device continuity, as well as GAN and diffusion artifacts to distinguish authentic user captures from synthetic or manipulated content. DocV evaluates frame-by-frame motion, liveness signals, and cross-session consistency detect sophisticated injection attacks. All signals can support high rates of accuracy with 98.7% fraudulent attempts detected and a 98%+ automated decision rate.

In addition, **Socure's** user-centric DocV solution includes accessibility features for visually impaired users and supports WCAG 2.1 AA standards, addressing consumer concerns often presented by typical document and biometric verification solutions.

Socure's DocV delivers verification responses in under one second, compared to the industry average of more than 30 seconds.

Socure Account Intelligence provides real-time verification of bank account status andownership across financial institutions, fintechs, credit unions, neobanks, alternative payment platforms, and more.

Socure

With coverage up to 98% bank account status and up to 82% bank account ownership coverage — it enables businesses to verify bank accounts in two seconds or less using only a name, account number, and routing number.

Beyond verification, **Socure** leverages cross-industry intelligence and first-party fraud signals to identify repeat bad actors who use their own bank accounts to exploit systems before transactions can occur.

For more information, visit www.socure.com

ArkOwl

ArkOwl is a real-time data provider offering email address and phone number verification. Using only an email address and a phone number, they provide 83 unique data points to help identify fraudulent patterns and activity. This functionality can help minimize fraudulent attempts while maximizing ability to identify legitimate users. They process over 14,000,000 transactions annually. Available data is 100 percent live in real-time. No data is pulled from stale, potentially outdated databases. Privacy is taken seriously with all data requests anonymized as requested through **ArkOwl**, so various providers of the data points seen in **ArkOwl** cannot track information on customers. To keep customer data absolutely private, they do not store any in the first place. Because the data is aggregated and presented in real time, there is no need to depend on storing and sharing data from customers. In addition, all connections are secured with 256-bit encryption.

ArkOwl provides users with aggregate profile data from several social media sites, webmail providers, domain databases, and other open data sources to gain insights into any email address or phone number. Clients can run hundreds or thousands of queries at a time through direct integration with an existing fraud detection platform, or by utilizing their new batch query system. Through the platform, **ArkOwl** automatically detects and highlights information needed for email validation and phone verification. This includes knowing whether an email address and phone number are linked to each other, real names, known aliases, registration status with popular service providers, and associations with any known data breaches through connecting with Haveibeenpwned.com.

At a Glance:

3rd Party API Capabilities

Professional Guidance/Services

Pre-Authorization Functionality

ArkOwl chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Ekata by Mastercard

Ekata by Mastercard is positioned to unify the elements of digital identities such as name, email, phone, IP address, physical address--creating one secure, trusted source of truth that delivers greater confidence in decisioning without sacrificing user experience. This is done with **Ekata's** identity verification data, or the Identity Engine. It is what powers all of the solutions- transforming billions of data into unique and valuable insights that allows businesses of all shapes and sizes to make accurate risk decisions about their customers.

- The Identity Engine comprises of two distinct & mutually exclusive data sources. We use these two data assets, apply our data science to produce our solutions that get integrated into your decision platform, rules engine, and most often today into models.
- Identity Graph is our 3rd party sourced database that validates the 5 key identity elements of name, email, phone, IP and physical address and how they are connected to each other.

Identity Network analyzes patterns of how consumers information is being used in digital interactions with behavioral patterns and transaction-level intelligence.

Ekata digital identity verification data builds trust by solving two types of challenges:

1. Digital onboarding: Increase passive authentication, mitigate synthetic ID fraud, onboard thin-file and unbanked
2. Payment fraud: optimize customer experience, increase approval rates, stop fraud early in the workflow

ekata by

At a Glance:

3rd Party API Capabilities

AI Powered

Pre-Authorization Functionality

Exata chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Emailage

Emailage, is a global risk management and fraud detection technology company. They help businesses deter online fraud and aid in the delivery of low-friction customer experiences through key partnerships, proprietary data, and machine-learning technology. **Emailage's** Fraud Detection and Risk Decisioning Solutions build a multifaceted profile associated with a customer's email address and renders predictive scoring for email risk, digital identity, and risk decisioning confidence. **Emailage** solutions are available through direct integration as well as partner channels. **Emailage** partners include Accertify, CyberSource, Equifax, Experian, and LexisNexis Risk Solutions.

Emailage is a corporate member of the International Association of Privacy Professionals (IAPP) and utilizes the Privacy Shield Framework. They completed their first independent third-party audit for SOC 2 in 2017 and hold registration number ZA138498 for the Information Commissioner's Office in the UK. All **Emailage** data centers comply with leading security policies and frameworks, including SSAE 16, SOC framework, ISO 27001, and PCI DSS Level 1.

emailage™
GLOBAL FRAUD PREVENTION

At a Glance:

3rd Party API Capabilities

Account/Client Management

AI Powered

Emailage chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Flashpoint

Flashpoint helps organizations prioritize intelligence, fill in the gaps, and focus attention on areas previously invisible. **Flashpoint** provides data across the Deep & Dark Web.

Flashpoint's Compromised Credentials Monitoring (CCM) allows users to monitor exposure of compromised credentials for their enterprise domains and customer email addresses. This lets them take action after breaches to mitigate risk of account takeover (ATO). **Flashpoint's** technology collects and processes data and credentials, allowing for organizations to access breach data and receive notification as soon as credentials have been identified. They also help identify accounts that have been compromised on a consistent basis in order to provide ongoing fraud monitoring without impacting user experience. Organizations can gain insight into the types of domains being targeted, as well as the most vulnerable passwords.

FLASHPOINT

At a Glance:

ATO Detection Capabilities

Pre-Authorization Functionality

Flashpoint chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

GB Group

GB Group (GBG) is a global data provider based in the United Kingdom. Two of their higher-profile clients include Etsy and Stripe. They state that they support their clients with effective identity data intelligence and that their data spans across the globe, specifically in 248 countries. **GBG** assists merchants in the following ways:

- **Managing Risk through ID Verification:** Their **MatchCode360** product builds out a profile including contact information and social IDs.
- **Fighting Fraud And Locating People:** With their **ID3Global** product, a merchant can perform identity management, checking that customers are who they say they are against records for more than 4 billion people in 26 major countries. They trace and identify fraudsters, transactional fraud, and fraud bureau (a retailer-compiled negative file of data).
- **Registering New Customers:** Achieved through data validation, enhancement, and streamline onboarding.

GBG

At a Glance:

3rd Party API Capabilities

GBG chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

GeoComply

GeoComply provides a reliable and accurate geolocation solution for fraud detection. **GeoComply's** solutions are based on the award-winning geolocation compliance and geo-protection technologies that **GeoComply** developed for the highly regulated and complex U.S. Gaming industry. The company's software is installed in over 400 million devices worldwide, putting **GeoComply** in a strong position to identify and counter both current and newly emerging geolocation fraud threats.

With technology proven and refined over 10 years of development and billions of transactions, **GeoComply** can accurately determine a users' true location and whether they are attempting to mask their location using various spoofing tools. **GeoComply** enables a wide range of industries including banks, fintechs, and cryptocurrency exchanges to detect and guard against geolocation-based fraud.

Four typical use cases for **GeoComply**:

- Onboarding & Account Opening
- Transactions Fraud Mitigation
  - AML and Sanctions Compliance
  - Ensure compliance with jurisdictional requirements by verifying the true location of a transaction.
- Authentication and Account Protection
  - Monitor account updates and user behaviour by adding geolocation checks to continuous authentication and protect against account takeovers and account update fraud while reducing friction.

GEOCOMPLY

Empowering The Future Of Digital Trust

At a Glance:

GeoComply chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Intent IQ

Intent IQ is an identity resolution solution provider that enables its partners to confidently identify clients and prospects who interact with their sites, apps, and brick-and-mortar establishments, across their various screens and in person. Their solutions identify site visitors and app users in multiple environments.

Verticals utilizing their products and services include ecommerce, financial institutions, and the media ecosystem. **Intent IQ** products and technology are backed by over 150 granted patents. Vectors of focus include account takeover and new account fraud. For ecommerce and financial institutions, **Intent IQ** validates a device user's claimed identity credentials. It checks whether the given device matches the devices of the claimed identity home by comparing different parameters that are difficult to mimic. The home is located by **Intent IQ** using the claimed identity postal address converted to latitude/longitude and claimed email.

Utilizing over 20 billion online ad-related signals every 24 hours and over 10 billion email open and log-in events every month, **Intent IQ** is able to create and maintain an accurate real-time map of U.S. and Canadian devices, their users' identities, and the relations amongst the devices. Relations include identifying the different devices owned by one person, as well as other people and their devices who share a home or office with that person.

At a Glance:

3rd Party API Capabilities

ATO Detection Capabilities

Pre-Authorization Functionality

Intent IQ chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

LexisNexis Risk Solutions

LexisNexis Risk Solutions is a US-based data provider with a repository of information covering 95 percent of US consumers. They can link and cross-check to reconcile name variations, duplicates, multiple addresses, and myriad other inconsistencies and linkages. This helps a merchant to:

- **Validate:** Confirming name, address, and phone information.
- **"Red-flag":** Identifying inconsistent data elements.
- **Perform Global Identity Checks:** Using integration and reporting capabilities.

Their data can validate individual addresses, confirm if there's a logical relationship between "bill-to" and "ship-to" identities, and assess transaction risk. They can identify risks associated with bill-to and ship-to identities with a single numeric risk score, detect fraud patterns, isolate high-risk transactions, and resolve false-positive and Address Verification Systems failures.

Their products allow a merchant to dig deeper to prevent fraud and authenticate identities using knowledge-based quizzes. Merchants can also adjust security levels to suit risk scenarios and receive real-time pass/fail results. **LexisNexis** also states that their identity verification and authentication solutions provide reliable verifications and increased sales while mitigating fraud losses.

LexisNexis® RISK SOLUTIONS

At a Glance:

3rd Party API Capabilities

LexisNexis Risk Solutions chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Oneytrust

Oneytrust helps organizations secure their business and boost the customer journey. They identify the customer profile as quickly as possible by analyzing the order data and assigning it a pre-score.

- Upon the validation of the basket, users detect fraudulent payment attempts and offer payment by credit card or in one click to other customers.
- The investigation is continued in order to secure the transaction as much as possible and make the right decision. Finalize your orders without any impact on the purchase tunnel even for high baskets.
- Device Fingerprint identifies the connected device to your site by collecting dozens of pieces of information (browsers, plugins, screens, language). This collection is transparent for the user and does not slow down his experience on the site.
- Virtual Investigator uses the data provided by the client (such as email, phone, address) to perform automatic research to determine a reliability score of a profile.
- Finally, a team deals with major risk transactions. Its objective is to investigate the operating modes in order to verify that the customer is at the origin of the order.

oneytrust

At a Glance:

Oneytrust chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Pipl

Pipl is the identity trust company. They make sure no one pretends to be you. They use multivariate linking to establish deep connections among disparate identifiers—email, mobile phone, and social media data that spans the globe—and then look at the big picture. **Pipl's** identity resolution engine continuously collects, cross-references, and connects identity records to create data clusters across the internet and numerous exclusive sources. **Pipl** uses machine learning and data analytics on its index of billions of trusted identity profiles to derive trust signal scoring that customers can leverage in their processes.

Pipl's customer is the digital consumer, and its products and services are industry agnostic. Some of the world's most prominent companies work with **Pipl**—in banking and finance, ecommerce, government services, insurance, law enforcement, media and journalism, sales and marketing, and more. **Pipl** provides them with frictionless customer experiences and approves more transactions while reducing chargebacks and the risk of fraud.

At a Glance:

3rd Party API Capabilities

Professional Guidance/Services

Pre-Authorization Functionality

Pipl chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

TeleSign

TeleSign supports 21 of the 25 largest internet properties and offers solutions including internet, social media, finance, gaming, on-demand services, and ecommerce. They are one of the few industry players to offer both communication and global identity solutions.

TeleSign is best known for API tools for security, authentication, fraud detection, and compliance scoring, connected to Communication Platform as a Service (CPaaS) voice, SMS, RCS, and WhatsApp. Go-to-market is primarily driven by TeleSign's own enterprise sales team and channel partners; clients have the option of a self-serve portal.

TeleSign risk solutions help organizations focus on bad actors who create online and mobile application accounts that result in spam, phishing attacks, promo abuse, and other costly fraud. In addition, by registering fake accounts, fraudsters can attack legitimate users and damage a brand's value, revenue, and growth. **TeleSign** helps organizations effectively identify and block these harmful users at account registration, while streamlining the process for authentic and valuable users.

TeleSign helps organizations focus on issues such as chargeback reduction, cost management, and fake account reduction within the following verticals:

- Financial Services
- Gaming
- Ecommerce
- Social Networking
- On-demand Services

TeleSign

At a Glance:

ATO Detection Capabilities

Account/Client Management

Pre-Authorization Functionality

TeleSign chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

TransUnion

TransUnion TruValidate™, now with **Neustar®** fraud solutions, orchestrates behavioral, device, and identity insights to help organizations secure trust across channels and deliver seamless experiences for consumers. Not only can companies increase trust at each stage of the customer journey and across channels—they can also improve customer conversion, reduce fraud losses, and enhance consumer satisfaction.

TransUnion leverages an authoritative network of physical, digital, and device identity data, including sources from transactional data, marketing footprint data, customer CRM data, MNO carrier device data, device consortium data, and credit header data. The **TransUnion** identity intelligence network is a repository of online, offline, and call center data that's broken down, corroborated, and rebuilt up to every 15 minutes. It's powered by an always-on network of partners' proprietary data sources with direct consumer relationships, including billing, telecom, and government agencies. The network effect of the **TransUnion** identity intelligence network allows for greater accuracy and breadth of omnichannel fraud and risk insights.

Solutions and functionality

TruValidate solutions distinguish safe from risky interactions through best-in-class signals and scores, providing a unified view of fraud and identity risk across online, offline, and call center channels for superior performance against key client KPIs. TruValidate comprises four primary product pillars that protect brands from fraud losses while helping to deliver friction-right customer experiences:

At a Glance:

3rd Party API Capabilities

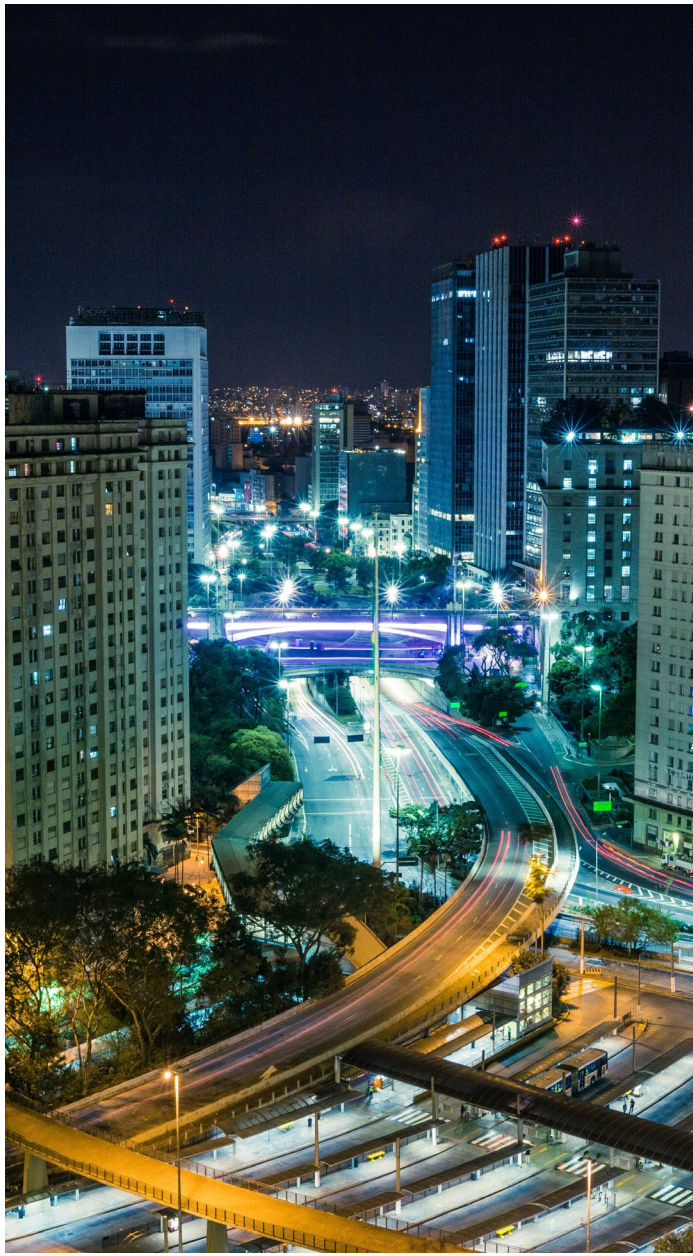
AI Powered

Account/Client Management

TransUnion chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Chargeback Management & Platforms

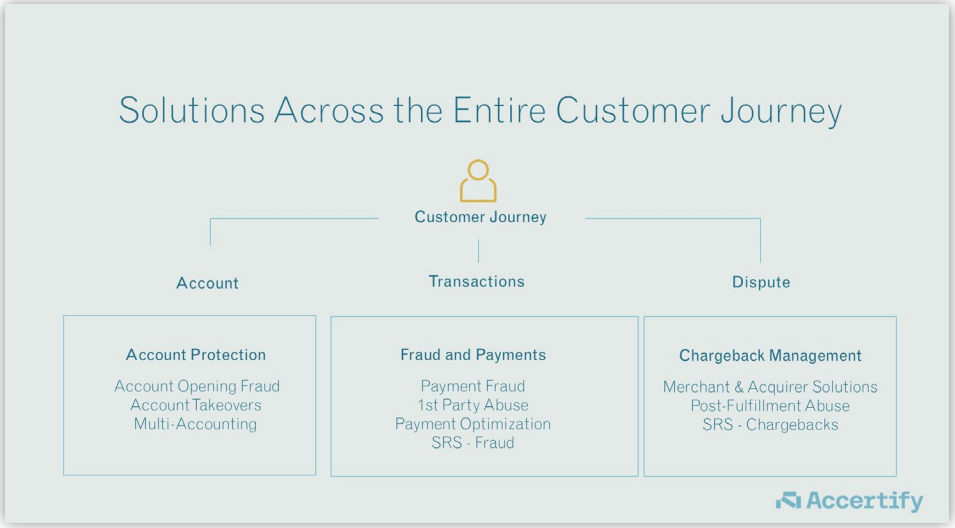
Chargebacks are just one of the many risks that threaten a business's success, but they also happen to be the most dangerous. If left unchecked, chargebacks steal profits and threaten a business's longevity. These solution providers can help increase your chargeback representment win ratio while lowering the cost of chargeback management. The breadth of services can range widely—some services simply provide tips on how to address inbound chargebacks, while others offer fully outsourced and fully integrated options. And many offer everything in between. These services blunt the overall impact of chargebacks whether the fraud is classified as malicious, friendly, affiliate, or otherwise.



Accertify Chargebacks

Accertify understands that customer expectations are ever evolving and so is fraud. Today's online consumers expect to be recognized and rewarded as loyal customers. They want to transact with a single click from any device and feel confident their account is secure. At the same time, each online event exposes your organization to reputational and financial risks that can have a material impact.

Trusted by many of the largest companies globally, **Accertify** is a leading digital platform assessing risk across the entire customer journey, from account monitoring and payment risk to refund fraud and dispute management. Accertify built a comprehensive platform with integrated solutions across the entire customer journey, letting organizations see the complete picture and proceed with confidence. **Accertify** can help reduce the need to juggle multiple vendors and decipher fragmented risk scores that result in unwelcome friction for customers.



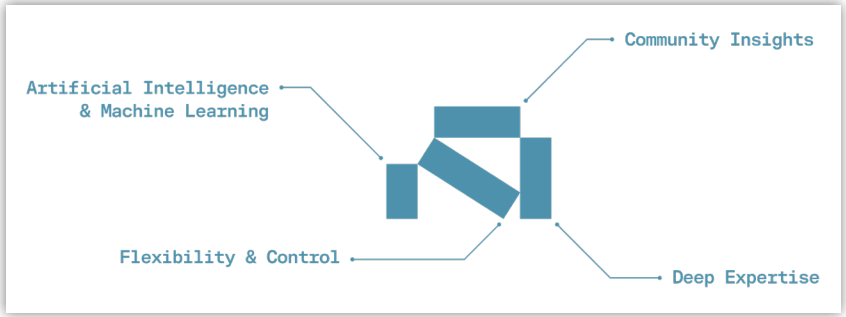
At a Glance:

- Operational Support
- Payment Gateway Capabilities
- 3rd Party API Capabilities
- Professional Guidance/Services
- AI Powered
- Pre-Authorization Functionality
- Fraud Engine/ Platform Functionality
- Account/Client Management
- Historical Sandbox Testing

Accertify Chargebacks

Accertify serves your risk strategy and business objectives with:

- Artificial intelligence (AI) and machine learning
- Community insights from global network
- Significant level of industry knowledge
- Flexibility and controls that adapt to suit clients' needs



Accertify® Chargeback Management Module

Unlike competitors offering black box solutions that rely solely on algorithms, **Accertify's** solutions balance the power of artificial intelligence with human intelligence.

Accertify offers a Chargeback Management Module that has been live and processing chargebacks since 2011.

Accertify is a Payment Card Industry Data Security Standard (PCI DSS) Level 1 validated service provider and SOC 2 compliant.

The Chargeback Management Module can be used either as a standalone product or in conjunction with **Accertify's** Fraud platform.

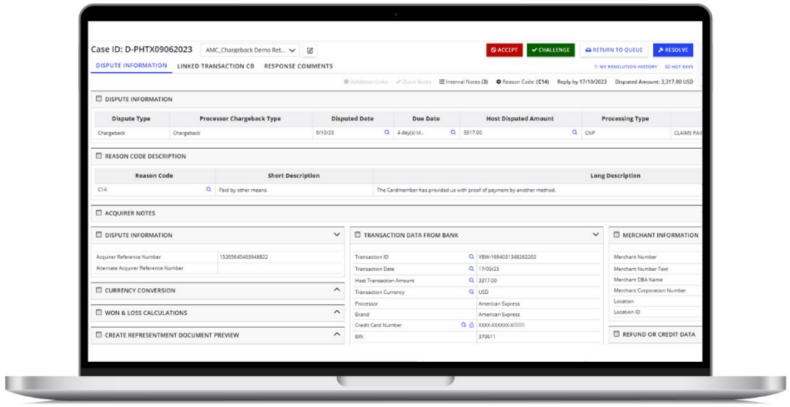


Figure 1: user interface

Accertify's Chargeback Management Module can reduce or fully remove the manual resources required to manage and respond to chargebacks by incorporating full or partial automation into the process. It offers a software-as-a-service platform that can be automated, manually managed by the client, or outsourced using Accertify Strategic Risk Services offering it. It is designed to meet merchants where they are on their current technology journey and allows them to evolve that journey as it fits within their roadmap.

Accertify Chargebacks

The platform offers:

AI and ML Capability: Accertify takes a technology-first approach using cutting-edge machine learning and AI technology to help manage chargebacks. The machine learning models consider chargeback data, purchase data, client history, and consortium data while incorporating the specific regulations from the card brands and the merchants' specific business policies to make the best decision about how winnable a chargeback is. Couple this with the use of AI technology to produce supporting documents, which focus on and highlight the pertinent information for the issuer, and you have an AI/ML human-led platform that automates and improves the entire chargeback process.

Automated Processor Integration: Accertify is integrated directly with most processors. This functionality allows for the majority of chargeback files to be automatically and systematically imported into the platform. In addition, chargeback responses can be automatically exported to integrated processors using similar technology.

Workflow Management: The platform has out-of-the-box workflows that help merchants manage chargebacks and chargeback-related procedures. It can create client-specific workflows based upon dollar values, chargeback reason, due date, client business needs, and other similar data points. It highlights the most important chargebacks to be worked on based on industry and client requirements. Examples of this include chargebacks on future flights, high dollar chargebacks, VIP loyalty customer disputes, most likely to win, etc.

Carrier Integration: This allows the user to quickly check the status of a delivery that was shipped to a consumer. This can be done manually, or it can be fully automated, streamlining the pulling of the proof of delivery information needed in the representment process. This integration works with over 1,000 shipping providers globally.

User Interface/User Experience: The user interface is always available, even in a full or partially automated setup. This access provides a way to manually include documentation via upload or copy/paste, and it provides a repository for supporting documentation and compelling evidence for representment. This ensures a full suite of capabilities to handle both full and partial automation and manual intervention needs without sacrificing accuracy or efficiency.

Web-Based Dashboards and Reporting: The reporting platform delivers end-to-end visibility into chargeback operations, empowering merchants to monitor performance, identify trends, and optimize team productivity. With interactive dashboards, detailed analytics, and secure data export capabilities, clients gain actionable insights to improve success and streamline workflows.

Accertify Chargebacks

Trend & Insight Reporting

The reporting package provides a big-picture view of chargeback operations through intuitive dashboards.

- Landing Page Dashboards: Show trends for items yet to be decisioned, recently worked items, and a 12-week or 12-month win/loss analysis.
- Deadline Monitoring: Highlights chargebacks nearing reply-by dates and recent work activity, helping merchants manage inventory and stay on top of timelines.
- Future Activity Identification: Highlights of chargebacks related to events in the future such as travel, event ticketing, and pre-orders.
- Trend Analysis: Data can be grouped by reason code, brand, and processor to identify patterns and inform strategy.

Analyst Performance

The platform enables detailed evaluation of team productivity and success if required:

- Filter Options: Users can select filters such as load/resolution/sale date, agent identifier, and reason code group.
- Performance Metrics: Win/loss success ratios are displayed by dollar amount, case count, and percentage for manually reviewed cases versus total accepted cases.
- Work Duration & Interaction Tracking: Shows who last interacted with a chargeback and calculated average work duration for a specified period.

Integration with Clients Business Intelligence Tool

For advanced analysis and internal reporting, the platform offers secure data export capabilities:

- Customizable Extracts: Clients define the data to be extracted and run it immediately or schedule it for later use.
- Seamless Integration: Enables merchants to leverage their own business intelligence tools for deeper insights and reporting.

Solution Integration

Accertify Chargeback Management Module is directly integrated with the Fraud platform, and information is automatically populated into the **Accertify** Chargeback Management Module and vice versa. The Fraud platform and Chargeback module form a symbiotic relationship. They seamlessly leverage and benefit from one another by staying synchronized and realizing their maximum potential through direct data sharing.

Accertify is seeing an increase in users seeking a vendor that supports an overall fraud strategy that includes both a chargeback management solution and a fraud detection solution. A rapid feedback loop from chargeback management is a critical

Accertify Chargebacks

component of the fraud strategy. Having a more closely integrated fraud and chargeback management solution can lead to more optimized fraud outcomes and (in many cases) improved win rates. Vendors that handle both fraud prevention and chargeback management create a feedback loop:

- Fraud signals inform dispute strategies
- Dispute outcomes refine fraud models – only solution providers with integrated chargeback and dispute solutions on the same platform have access to the "truth" they need to update models in real-time
- Friendly fraud chargebacks have become easier to spot

When combining fraud and chargeback management with the same vendor, dispute win rates typically improve. This is because a strong fraud strategy reduces fraud-related chargebacks (which can be difficult to win), shrinking the denominator, and boosting overall win rate.

If you are not a Fraud client, **Accertify** supports direct integrations to merchant CRM systems, which allows the platform to provide the same level of automation and data as our joint solution provides.

Accertify also partners with Ethoca, Verifi, and American Express to enable pre-chargeback capabilities related to dispute deflection, transaction clarity, and chargeback alerts. This allows clients to react to change faster, including potentially avoiding the chargeback by stopping shipments, issuing refunds, improving fraud prevention rules and strategies, and enhancing model performance. If executed effectively, this strategy can be applied while providing an enhanced customer experience.

Chargeback Gurus

Chargeback Gurus (CBG) is the leading automated AI-orchestrated chargeback management platform, helping merchants protect and recover more revenue. **CBG's** solutions are powered by sophisticated technologies, rich analytics, and deep industry expertise.

CBG's chargeback management platform provides real-time insights, predictive analytics, and comprehensive reporting to help merchants stay ahead of evolving chargeback challenges.

Their solutions combine automation, AI, and deep industry expertise with configurable sophisticated technologies to deliver hundreds of millions of dollars in recovered revenue to clients. The platform offers support in optimizing a range of KPIs, including:

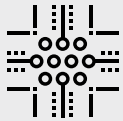
- Revenue protection
- Bad debt reduction
- Recovery (win rate, recovery amount, recovery rate)
- Chargeback health and prevention (chargeback ratio, alert and Order Insight deflection, fraud ratios, VAMP ratio, and MID health)
- Operational efficiency and quality (Turn Around Time (TAT), Work In Progress (WIP), productivity, analyst/supervisor performance, evidence quality score, ageing analysis, and winnability

CBG serves many of the largest and most recognizable brands in the world and works within all major industries, including hospitality, marketing and advertising, car rental, retail, entertainment, telecom & media, health, wellness & fitness, subscription, and insurance.

At a Glance:

3rd Party API Capabilities

AI Powered



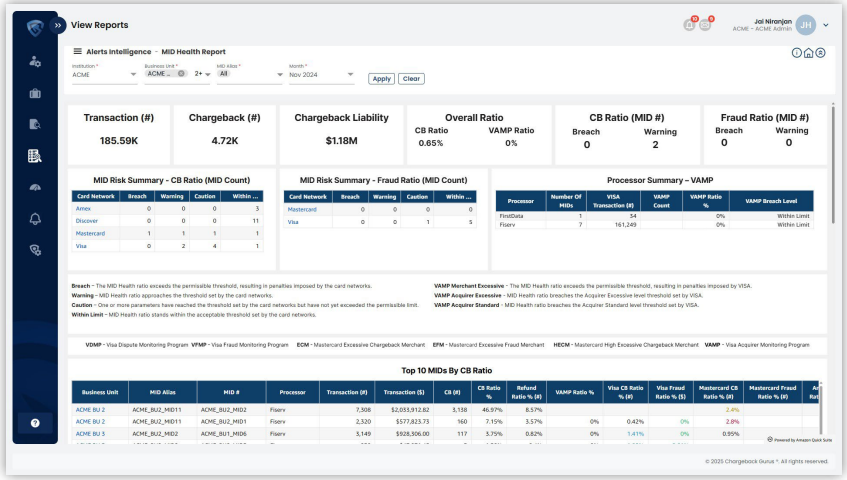
Non-Production
Real Time Rules Testing

Fraud Engine/
Platform Functionality

Chargeback Gurus

Their collaborative approach offers flexible, custom solutions to each merchant and their specific goals and challenges. Through iterative processes, they take an adaptable, constantly evolving approach. This includes industry-specific Customer Data Platform (CDP) frameworks, feedback loops, and A/B testing to optimize outcomes. A white-label model with multitenant Partner Management and cobranding/white-label capabilities also exists.

CBG offers a Chargeback Profile Analysis as a proof of concept, in which **CBG** processes a prospective client's historical data through the **CBG** platform to simulate "what-if" scenarios and quantify potential improvements in win rate and recovery, along with reductions in chargeback exposure, before launch. This enables data-driven ROI projections and risk-free evaluation of the solution.



Technology / Product:

CBG address both pre-dispute and post-dispute categories through Self-Service, Managed Services, and SaaS offerings:

Managed Services (CBG-operated):

- Smart Chargebacks (Representment): **CBG** fully manages chargeback disputes and evidence submissions to maximize recovery.
- Smart Alerts (Prevention & Early Resolution): Proactively resolving disputes before they become chargebacks leads to loss reduction.
- Order / Order Intelligence (OI): Real-time access to detailed order and transaction data helps issuers and merchants resolve disputes faster, reduce chargebacks, and improve customer experience through enhanced data transparency.

Smart Dispute Solutions (Client- or Merchant-operated):

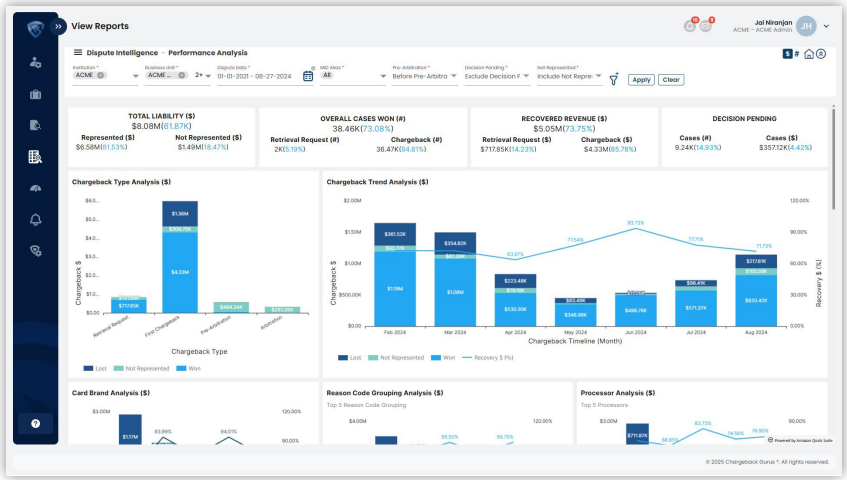
- Smart Dispute Alerts: SaaS self-service alert management, guided refund workflows, and integrations with Verifi/ Ethoca/Amex/Paypal.
- Smart Dispute Solutions: SaaS Self-service platform manages chargeback cases and evidence.

For **Stripe** users, a **Marketplace App** also exists:

- Plug-and-play app for Stripe merchants enables Prevention Alerts workflows with minimal setup.

Reporting options available, include:

- Standard Analytics: Executive Summary
- Smart Enhanced Analytics: Performance Analysis, Root Cause analyzer
- MHR + Custom Notifications: MID Health Report with tailored alerting/notifications for thresholds and anomalies
- Descriptive Analytics
- Ad hoc: Client-specific analyses and custom reports available on request



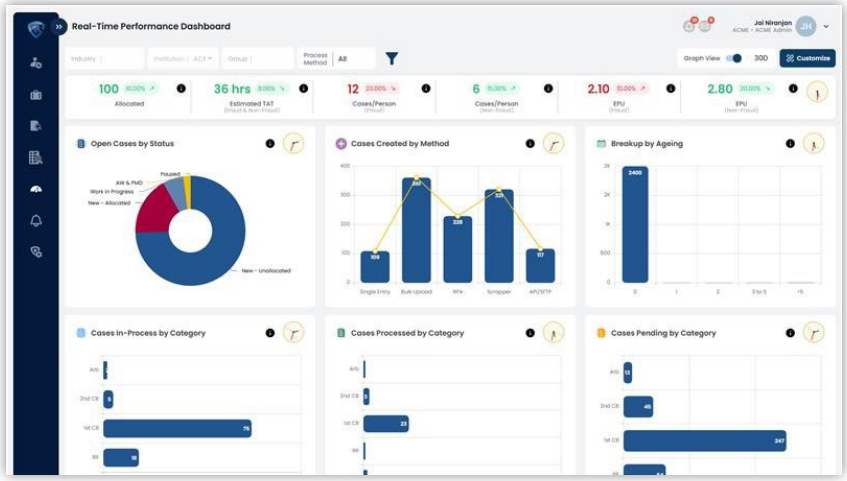
Integration options:

Regarding full integration post proof of concept, **CBG** aims to "meet its clients exactly where they are technologically." The platform is flexible with integration methodologies and no-code/low-code solutions, when needed. The solution is also offered through several third-party partnerships.

CBG offers API specs for integration which can either be push-based or pull-based. Details are shared with clients and customized on a contract basis. The typical timeframe from signature to launch is 3-6 weeks.

- Modern APIs & SDK:
  - Onboarding API Suite – Users and Merchants/LOBs/MIDs, Service Setup
  - CB Prevention – Integrations with CRM systems to manage refunds
  - CB Representment – APIs to ingest Chargeback, Transaction, Order/CRM data
- Network/provider integrations: Visa, Verifi, Mastercard, Ethoca, Amex , 40+ processors/acquirers
- Robotic Process Automation (RPA)/automation where APIs are unavailable, with centralized bot control

Chargeback Gurus



Support options once integrated:

- Tiered support: L1–L3 with defined escalation; email/portal workflows; configurable SLAs
- Consulting Services: Supported by its data science practice and dispute expertise, **CBG** provides consulting for both managed services and the SaaS solutions to help its clients become better business operators and service providers
- Training Services: Comprehensive training ensures teams master both basic and advanced platform features
- Industry-Specific Customization: Services tailor evidence, data fields, and dispute frameworks to align with specific industry needs
- Integration Services: **CBG** provides secure API/SFTP integrations for user management, evidence, and case data, plus certified connections to third-party alert/dispute networks, speeding up onboarding and improving data quality
- Client Specific Customizations: **CBG** customizes fields, sections, evidence, CDP frameworks, and dashboards to match client's operating model, with optional white-labelling to align with brand guidelines and boost efficiency

Pricing format:

CBG offers its clients flexibility regarding compensation models. Clients most commonly choose a per-unit model, a performance model, or a hybrid of the two.

Road Map:

- Key developments on the calendar for the next 12 months include:
- AI-powered Alert Refund Decisioning Automation
- Evidence Validation (type and content)
- Win/Loss Analyzer
- Multilingual capabilities and vertical workspace enhancements
- License management for SaaS
- Agentic AI-driven automation to further transform dispute and alert management

ChargeBacks911

ChargeBacks911 (sometimes called simply "**CB911**") primarily provides fraud chargeback management for merchants and contributes to loss prevention efforts of their merchant clients. **CB911** also states that they include an return on investment (ROI) guarantee as part of the chargeback management platform.

They state they have the following capabilities as part of their solutions:

- **Affiliate Fraud Detection:** Via proprietary technologies and personalized analysis, **CB911** lets merchants identify marketing campaign threats created by illegitimate affiliate marketing ploys.
- **Source Detection: CB911's Intelligent Source Detection** is described as their own blend of patent-pending technologies and expert human analysis designed to identify the true reason for a chargeback.
- **Merchant Review: Merchant Compliance Review** offers insight into merchant processes and identifies steps to reduce chargebacks and increase re-presentment win rates.
- **MAC Reporting:** This gives a merchant the ability to monitor their credit card processing charges, and it helps identify unjust expenses.
- **Chargeback Re-presentment:** Via the **Chargeback Tactical Re-presentment** product, this guarantees profitability by winning re-presentment as well as identifying more potential dispute opportunities.
- **Chargeback Alerts: CB911** combines a proprietary solution with solutions from third-party providers like Ethoca Alerts and Verifi CDRN to be alerted of chargebacks before they happen.

CB911 received the Card Not Present (CNP) customer choice award in 2016 for Best Chargeback Management Solution.

At a Glance:

CB911 chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

ChargebackOps

ChargebackOps was founded in early 2015 to combat the notion that chargebacks are an inherent cost of doing business. Their approach focuses on making use of the broad amount of data provided by chargebacks. They help clients leverage these details to not only reduce chargeback losses but also help better manage customer service issues, improve automated decisions, and reduce manual reviews.

ChargebackOps offers two primary services:

Chargeback Management Service: **ChargebackOps** offers a uniquely designed dispute resolution service for Fortune-500 ecommerce companies who prioritize the lifetime value of their customer and their brand. Using a hands-on and collaborative approach, their analysts investigate and respond to each chargeback case in order to optimize the client's desired handling for all types of fraud.

Order Screening and Review Service: **ChargebackOps** provides a cost-effective multi-platform order review service for ecommerce and buy-online-pickup-in-store (BOPIS) programs. Using client-dedicated review analysts, **ChargebackOps** typically out-performs their client's internal screening teams, or other third-party outsourced teams. Their service combines human intelligence with a custom-built application to provide analysts with better fraud insights for fast, reliable, and effective decisions.

They review and cross-reference over 30 data points to provide a conversion rate better than 90%. The expert teams become an extension of a client's internal fraud and customer service teams, helping them exceed their fraud goals at an optimized price.

chargebackops

At a Glance:

ChargebackOps chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Ethoca

Ethoca is a collaboration-based fraud and chargeback prevention company founded in 2005. Originally founded as a merchant-to-merchant data-sharing solution, **Ethoca** pivoted in 2010 to launch **Ethoca** Alerts. Alerts was the result of a conversation with a large U.S. issuer who wanted to bypass the chargeback process and eliminate any communications latency between issuers and merchants—providing reciprocal value to both parties.

The aim was to give merchants immediate access to confirmed fraud data and customer dispute data, providing a window of opportunity to stop the fulfillment of goods (avoiding settlement where possible), or refunding the cardholder directly to avoid the impending chargeback. **Ethoca's** view is that, for both bank and merchant, this collaborative approach creates a better customer experience, since in many cases the arduous claims process can be avoided and the dispute can be resolved during the first contact with the customer.

Ethoca Alerts is a value-based service, and clients are billed based on performance. In April 2019, **Ethoca** was acquired by Mastercard, who intends to further scale these capabilities and combine **Ethoca** with its current security activities, data insights, and artificial intelligence solutions to help merchants and card issuers more easily identify and stop potentially fraudulent purchases and false declines.

ethoca™

At a Glance:

3rd Party API Capabilities

Account/Client Management

Ethoca chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Sift Dispute Management

Sift Dispute Management offers a web application that includes a set of APIs to retrieve data from various systems, aggregating them into a single interface in which to organize, build, and easily submit responses. **Sift** applies strategic automation and ML-powered intelligence to the process of creating chargeback responses, helping businesses to increase win rates and improve operational efficiency.

Within the Console, analysts are provided a queue that allows visualization of all disputes at every stage in the chargeback process. Analysts can utilize filters, analyst assignments, and customizable labels to boost team productivity. Within the Dispute page, analysts can view and dynamically apply category-based evidence instead of having to copy and paste from disparate sources. The solution is flexible enough to support a wide range of industry-specific evidence, allowing businesses to keep pace with the evolving requirements of each card network.

The Console provides a response generator, which can collect order, customer, transaction, and dispute data and add it to auto-populated responses. These responses address the specific requirements outlined in Visa, Mastercard, American Express, and Discover rules and regulations. Contextual evidence blocks are pre-scripted and auto-drafted. Merchants are then guided through any additional evidence application. These recommendations are provided through "tool tips" and are powered by machine learning. They ensure that optimal and applicable evidence is submitted by flagging key gaps and optimization opportunities. If there are certain types of evidence that are always applied in the same way, these can be automatically uploaded without additional user interaction.

sift

At a Glance:

Operational Support

Account/Client Management

Professional Guidance/Services

Sift chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

paladinfraud

Paladin Fraud would like to thank all of the participating vendors for their time and availability during the discovery and post-writing processes.

We also would like to remind all readers of this report that they can email us at info@paladinfraud.com to let us know which vendors they would like to see participate in the report next year.