paladin vendor report | **fraud prevention**

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 40 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 2022 Paladin Vendor Report

Offering an unprecedented view into today's fraud prevention platforms and solutions.

Every day at Paladin Group, we're in the thick of the fast-paced world of fraud solutions. This is especially important as the global pandemic has accelerated the use of digital environments at a level never experienced before. As malicious individuals take advantage of COVID19 and related scams, it's become even more important to remain focused on streamlining and maximizing the capabilities of an organizational fraud management operation.

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.

Since it's our mission to serve as an authority on these products and their strengths, areas of opportunity, and enhancements, 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 on an annual basis. And now, we're pleased to publish the latest: the 2022 Paladin Vendor Report. We've offered previous participants the chance to update their sections and incorporated additional participating vendors.

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 vendor's current 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 - The verticals vendors are focusing on and messaging
SALES - A breakdown of market segments.
TECHNOLOGY - How the product works from a technical perspective.

Introduction

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) and omni-channel 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 six 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 & Behavioral Biometrics**
- **3DS & Consumer Authentication**
- **Device Identification, Reputation, & Reputation**
- **Fraud Platforms & Decision Engines**
- **Identity & Data Verification**
- **Chargeback Management & Platform**

Introduction

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.

Machine Learning – 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.

DataVisor

DataVisor is a comprehensive fraud and risk management platform powered by transformational 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. With fast and easy integration and rapid time to value, **DataVisor** delivers solutions focused on high detection accuracy with lower TCO to reduce the cost of fraud. **DataVisor** protects global clients across digital commerce, fintech, marketplaces, travel platforms, and financial services against financial loss.

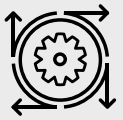
DataVisor supports complete account lifecycle protection starting with account opening fraud, payment and chargeback fraud, ATO, promotion and policy abuse, application fraud, transaction fraud, AML and more. Verticals of focus include financial institutions, fintech, travel, insurance, digital commerce, 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.

Solutions and Functionality

The **DataVisor** fraud detection solution takes a multi-pronged approach. Unsupervised Machine Learning (UML) detects unknown fraud, Supervised Machine Learning (SML) and rules capture known fraud, device intelligence combats mobile attacks, a feature platform derives intelligence from data, and a Knowledge Graph offers visualized linkages while supporting increased efficiency.

At a Glance:



Machine Learning

User Behavior Capabilities

Pre-Authorization Functionality

DataVisor

DataVisor provides Rules Engine, where clients and partners can create and manage business rules and decision flows with built-in simulation and real-time rule performance analysis. It also supports creating advanced fraud features to enhance rules and run backtesting on extensive historical data.

Data Integration options support internal and third-party data from omni-channels in real time or in batch. Accelerate data cleansing and ETL for rapid model development and decision making. In addition, users get out-of-the-box fraud feature packages to jump-start protection. The function gives organizations the ability to analyze large sets of data to create production-ready features via UI or coding without IT dependency.

The **Decision Management** allows for handling of business rules and decision flows with built-in simulation and real-time rule performance analysis.

Case Management functionality provides alerts, supports analysis of cases, queue management and user access. It also supports bulk actions on fraud rings and auto decisions. Within the interface, users gain access to detailed reason codes and a full audit trail.

Native device intelligence that combines device signals with device behavior analytics identity and stop fraud at inception at a device level.

A newly launched Insight Center offer fraud management and stategists an analytics dashboard to proactively protect against fraud.

The platform supports an organization's ability to detect evolving and unknown fraud without reduced need for historical data, training labels and constant model retuning. Real-time detection capabilities allow for handling years of data for large institutions and processing of large amounts of data in real time.

Proof-of-Concept process includes:

- Define scope, timeline and commercial terms for trial.
- Align on use cases, technical requirements, stakeholders, and project schedule.
- Define data acquisition methods and solution approach.
- Provide and evaluate asset onboarding documentation.
- Define key performance indicators (KPIs) and success metrics for the POC.
- Align on kick off meeting and follow-up meeting cadence and communication methods.
- Test the drive platform with your data. Participate in Q&A, training, and expert-led discovery sessions.
- Evaluate value discovered during your hands-on POC experience.
- Discuss next steps (technical and commercial agreement).
- Finalize terms for full contract and sign.

DataVisor

Integration and support:
Integration includes both cloud and on-premises options. The integration usually takes less than two weeks and requires minimum effort and resources from the organization. **DataVisor** will provide a professional team to help with the onboarding process, along with comprehensive training and 24/7 support.

The integration efforts needed by (initial) implementation of the solution are covered by the contract with no extra charge. For post-onboarding additional needs, customers can purchase the "software engineer and integration related" hours and package. (These needs could include production phase, if the customer wants to add more data event types to the integration, or if the customer wants big changes in data schema.)

In general, DataVisor has three types of PS package available for customers to buy and add to the service:

1. software engineer and integration related
2. fraud strategies and data analytics related
3. machine learning model development and tuning related

The contract comes with a standard ongoing support package, including 24/7 support, a dedicated customer technical account manager, biweekly meetings, quarterly business reviews, and more.

SLA terms are provided for response time and resolution time for different tiers of issues. In general, for P0 (the most urgent) issues, the response time SLA is 30 mins. For P1 to P3 (important but not top-urgency) issues, the response time SLA is 24 hours, but this does vary between different clients and contracts.

In development over the next 12 months
Customizable Configurations and Workflows in Case Management: this includes the ability to customize and define various views through UI to investigate a case, advanced analytics capabilities on top of result tables and review status, charts and figure drawings, and report generation.

Neuro-ID

Neuro-ID segments fraudulent digital applicants from genuine future customers by harnessing powerful advancements in behavioral science. Via a lightweight JavaScript integration, **Neuro-ID** collects high-fidelity behavioral signals from web and mobile applications, then processes these signals, in-session, to inform real-time decisioning. **Neuro-ID** customers receive highly accurate scores ("**Neuro Confidence Scores**") and attributes ("**Neuro Attributes**"), thereby gaining deep behavior-based insight into every digital applicant. **Neuro-ID's** scores and attributes offerings are accompanied by an intuitive dashboard, giving companies insight into previously unknown end-user behaviors. These behaviors indicate intent—fraudulent or genuine—as well as emotion and experience during the course of a digital customer journey.

Neuro-ID helps support improvements of the following KPIs:

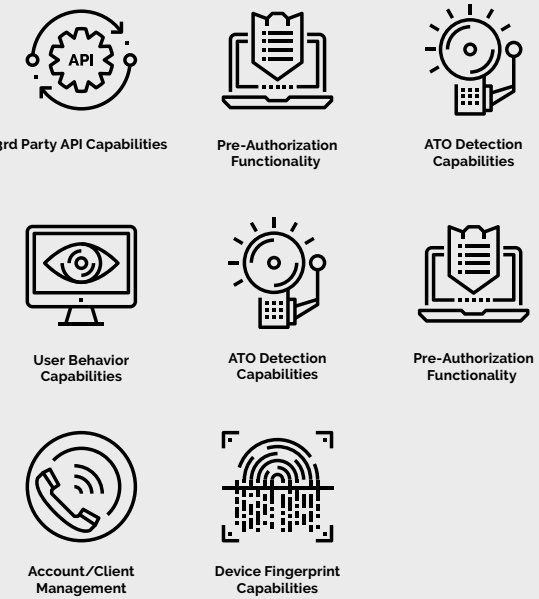
1. Fraud rate
2. False positive rate
3. False declines
4. Conversion rate

Neuro-ID operates in the digital onboarding environment, account creation, account management, and account access. They are expanding rapidly into ecommerce and have a successful history in lending, payments, buy-now-pay-later, and insurance. The technology helps organizations "optimize friction," which means that not only are bad transactions caught—but also, more good transactions are identified and accepted, supporting improved conversion and higher revenue totals.

Consequently, **Neuro-ID** moves risk management teams from cost centers to revenue generators and, in many cases, opens additional market opportunities that are

NEURO-ID®
HUMAN ANALYTICS™ FOR THE DIGITAL WORLD

At a Glance:



Neuro-ID

historically seen as high-risk. **Neuro-ID** is uniquely positioned to benefit both risk and experience teams: the future of behavior-based, scientific signal optimizes conversion while reducing risk.

Neuro-ID's data science utilizes sophisticated machine-learning models in order to generate these predictive scores and attributes, which help to separate risky end-users from genuine end-users. Scores and attributes are provided to customers to inform real-time decisioning. Customers generally build rules and policies around these scores and attributes based on business processes and objectives.

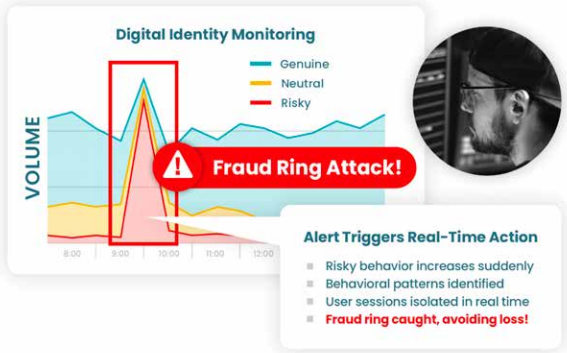
Neuro-ID is typically used as a layer in a larger stack. This helps organizations maximize their current investment in already-purchased fraud tools. These innovative organizations shift from making decisions based only on historical data to unlocking additional insight into digital behavior. **Neuro-ID's** first-of-its-kind "friction index dashboard" then helps these organizations measure and score customer friction and potential false positives. Behavior-based signal is not limited to only reducing fraud. By going beyond fraud and risk tracking, the dashboard provides insights for any internal team that cares about digital experience, including marketing, customer experience, and executive-level personnel. The friction index insights can indicate rates at which users leave the site, on which page, and which field—all the way down to session level.

As a real-time translation of "digital body language," **Neuro-ID's** proprietary scores and attributes reveal the "intent" behind behavior, also surfacing emotions of the online experience. **Neuro-ID** collects no Personal Identifiable Information. Its algorithms can help determine if a digital applicant is who they say they are entirely by analyzing in-session behavior. This serves as a critical additive and orthogonal signal that is independent of outside data sources. Because of this, **Neuro-ID's** technology is effective for first-time applicants and provides customers with day-one value.

Neuro-ID maintains 110 million consortium users, which are utilized to support construction of custom models, off the shelf insights, and a client-specific approach. Clients can compare and contrast their approach to what similar organizations are doing and benchmark their success across industry.

Reporting options: Reporting options with **Neuro-ID's** behavioral data include a behavioral dashboard, which shows both aggregate views of a customer journey and session-level insights for reviewing anomalous behavior. **Neuro-ID** also provides ad-hoc files for session-specific scores and attributes for deeper analysis.

Neuro-ID



Proof of Concept process: Neuro-ID's Proof of Concept process begins an assisted JavaScript integration. Reporting is made available via **Neuro-ID's** behavioral dashboard for understanding points of friction within a customer journey as well as behaviors indicative of fraud. Specific sessions are highlighted on a weekly basis for further analysis as part of the POC. **Neuro-ID** monitored 100M sessions in 2020, with a 500% year-to-year growth rate.

Pricing format: In order to ensure maximum benefits, **Neuro-ID** recommends passing as many transactions through the solution as possible. To support this, they work through a subscription-based pricing model with a flat monthly fee rather than a "per transaction" pricing structure. The maximized transaction volumes help increase accuracy and confidence.

Platform partners will utilize a flat fee in addition to a per-API call. This format will vary based on type of transaction but will maintain the focus on maximum visibility by passing as many interactions as possible. Further, this holistic approach supports the notion of monitoring not only fraud but also reducing friction for legitimate customers and account holders.

Integration:

Integration with **Neuro-ID** consists of implementing a JavaScript snippet for data collection. Additional integration with **Neuro-ID's** API enables retrieval of behavioral scores and attributes. Support for integrations is provided as part of customer onboarding, and there are integration guides for both the JavaScript and API integration. Level of effort for implementation depends on the capacity of the client but is typically completed within a couple of business days. **Neuro-ID's** integration experts routinely assist both large-scale enterprise organizations and small, nimble teams.

***integration docs linked in report?

12-month roadmap:

Over the next 12 months, **Neuro-ID** will invest in building out additional behavioral signals for various market use cases. They'll be working on third-party integrations for turnkey consumption of behavior-based intent and experience signals, and they'll be enabling data collection across additional channels aside from browser-based websites.

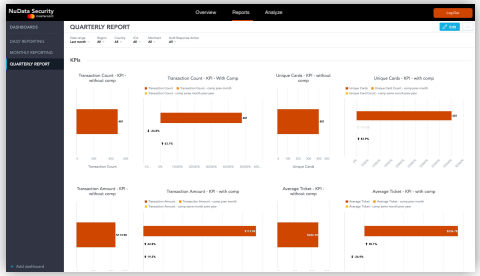
In addition, the upcoming fourth generation of Javascript will dramatically increase ease of integration.

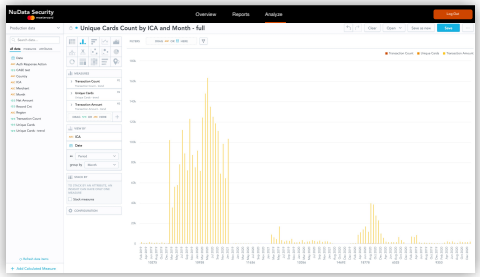
NuData

NuData Security, a Mastercard company, is an award-winning provider of behavioral biometrics and device intelligence solutions and is trusted by some of the world's largest brands across eCommerce, digital banking, and beyond. **NuData** helps companies stop account takeover, prevent new account fraud, and reduce unnecessary friction in real time.

With over 20 billion risk assessments and 4.5 billion devices processed yearly, businesses across the globe benefit from the power of **NuData's** Trust Consortium to validate good users without disruption and stop bad actors before they can cause damage.

The company's acquisition by Mastercard increasingly builds a world of online identities to recognize users beyond their credentials and personally identifiable information. As part of a globally trusted brand, **NuData** benefits from visibility into the Mastercard ecosystem. Recent developments include application of **NuData** technology into Mastercard's EMV 3DS transactions as well as performing behavioral biometrics during a OTP (One Time Passcode) to better support PSD2. Additionally, **NuData** technology has been integrated into Mastercard's Risk Based Authentication Engine (RBA) as well as integrations in support of Open Banking standards.





NuData continues to evolve to recognize growing attacks that involve coaching, human farming, social engineering, and remotely-accessed Trojan.

NuData Security

mastercard

At a Glance:

- Professional Guidance/Services
- Machine Learning
- Non-Production Real Time Rules Testing
- User Behavior Capabilities
- ATO Detection Capabilities
- Pre-Authorization Functionality
- Account/Client Management
- Device Fingerprint Capabilities

Solutions & Functionality

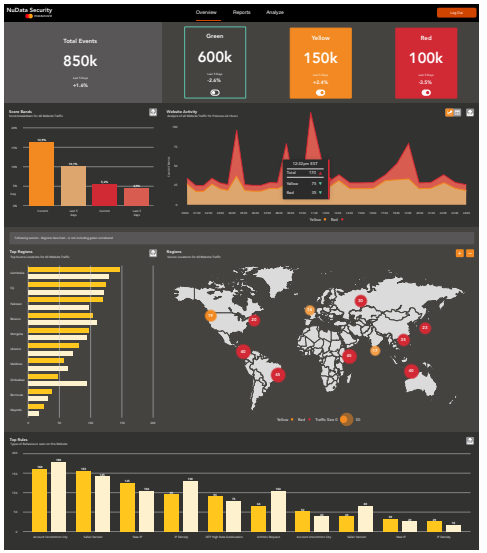
NuData looks at hundreds of data points with each interaction. Its technology builds an online user identity that recognizes users and protects them from fraud. This technology transparently looks at the user across different technologies integrated into one platform: device intelligence, behavioral analytics, passive biometrics, and the **NuData** Behavioral Trust Consortium—a pool of cross-client data.

NuData's technology and its **NuDetect** platform are offered as a group of solutions, each targeted to specific industry pain-points and use cases. As such, **NuData** offers specific solutions that protect from account takeover and other access attacks (**NuDetect** for Account Takeover). They also offer improved user verification (**NuDetect** for Good User Validation), device intelligence (Mastercard Trusted Device API), and cross-session security and monitoring (NuDetect for Continuous Validation). These solutions have a high impact on large and medium-sized businesses. **NuData** continues to identify potential use cases for new and unique business models.

NuData solutions cover the following use cases:
Account takeover: NuDetect for Account Takeover stops automated and human-driven attacks at login, even those that bypass bot-detection tools. It creates a risk score for each user in real time using behavioral biometrics technology. Companies can identify legitimate users, reduce friction, and keep accounts safe.

This can help clients by:

- Preventing attacks, scripted or human-driven, to access user accounts illegitimately
- Increasing trust in customer interaction
- Reducing friction for trusted customers



Account Creation Risk: The sheer amount of consumer data available to malicious users represents a nearly limitless resource for launching new account fraud. When fraudulent new accounts utilize legitimate identity data, verifying these accounts can be difficult. Through their four-layer approach discussed in this report, **NuDetect** for Continuous Validation evaluates whether a user is behaving like a legitimate user, like a fraudulent human user, or like a bot. High-risk accounts are flagged, so the appropriate steps can be taken.

This can help clients:

- Prevent future fraud from these accounts
- Reduce operational costs
- Flag human-farm-based account creation

NuData

Reduced user friction: Recognize your returning users with behavioral biometrics and analytics to remove unnecessary friction from your customer's online interaction based on their inherent behavior profile. By leveraging insights from NuData's trust consortium and device intelligence, NuDetect for Good User Verification can determine if a user is genuine, a human imposter, or bot.

This can help clients:

- Reduce false declines
- Remove unnecessary friction
- Create customized journeys

Coaching/social engineering: Coaching lures victims into sending money to the bad actor, where they coach the victim through the steps. Realize when users are behaving differently than how they normally do, even if you know it's them behind the device. Coaching victims are under pressure and their behavioral changes can trigger red flags to protect the legitimate user.

This helps clients:

- Prevent a fraudulent purchase or money transfer
- Increase trust of the client on the platform

Remotely-Accessed Trojan (RAT) prevention: Bad actors can take over a user's session and control their device to access a platform. Luckily, when this happens, the attacker's behavior is noticeably different than the expected user's behavioral patterns. This is how **NuDetect** for Continuous Validation mitigates these attacks before they create damage on the victim or company.

This helps clients:

- Confidently make risk decisions
- Protect user accounts

Checkout fraud protection: Card cycling and testing, a practice to know which stolen credit cards are active to use in a subsequent fraudulent purchase, has gone up. **NuDetect** for Continuous Validation helps companies mitigate this automated behavior at checkout before attackers can find out any information on their stolen cards.

This helps clients:

- Block attackers from a source of information
- Prevent subsequent fraudulent purchases

PSD2/SCA compliance: The new PSD2 regulation in Europe introduced Strong Customer Authentication (SCA) to reduce fraud and secure payments. In simple terms, SCA requires additional authentication steps built into the checkout flow.
NuDetect leverages behavioral biometrics and hundreds of data points from each OTP-completion to recognize trusted users. This fulfills two of the three SCA required factors: inherence (behavior)

and possession (device).

Device Recognition: A subset of the NuDetect technology focuses on recognizing risky and returning devices to prevent fraud as well as recognizing trusted users without added step-ups. This can be implemented as a stand-alone solution using the API, an option especially interesting for small and medium businesses.

The technology that supports the NuData solutions:

NuData uses a multi-layered approach to verify users online through traditional and behavioral methods. These layers work independently and together to identify anomalies, spoofing, or unexpected user behaviors and generate and share the gathered intelligence with our clients in real time.

The four layers include:

Device Intelligence

By gathering data points from device, network, connection, and location across the **NuData** network, the device intelligence layer creates a unique identifier. This allows clients to sort through traffic with ease and recognize devices more accurately than with traditional device recognition tools.

Behavioral Biometrics

How we type, hold a device, or move the mouse are unique to each of us. Our behavioral biometrics technology passively builds a profile by looking at those inherent movements made by a user without prompting any challenges.

Behavioral Analytics

Behavioral analytics combines data collected from the device intelligence and behavioral biometrics layers to behavioral profiles: a summary of how individual users and populations commonly behave. This profile is compared against past events to analyze events in real time and help clients accurately determine if the right person is behind the device.

Mastercard Trust Consortium

The Mastercard Trust Consortium is the world's largest network to assign risk scores to online events in real time. By gathering and analyzing anonymized data from opted-in providers, the Trust

NuData

Consortium uses historical risk factors, estimated trustworthiness, and reputational insights to assign a risk score to new interactions within milliseconds.

With billions of data points monitored annually, **NuData** clients benefit from the breadth of aggregated data and can prevent fraudulent attacks before they can cause damage.

AWS Private Link

NuData is also the option for "when the cloud is not an option." The company is recognized by AWS as PrivateLink Ready, a designation that allows **NuData** to offer its **NuDetect** product suite sending the data through a private connection instead of hosting it in the cloud, through the regular open internet. This offering is especially useful for companies subject to strict data protection regulations that can't process their data across the internet but still want to have a strong and real-time user verification process.x

How does NuData work?

Every time a user interacts with the app or web platform, NuData evaluates the user's inherent behavior and other data to build a score and make a decision in real time.

Components of that decision include:

- **Real-time scoring intelligence:** At each behavioral interaction, NuData generates a score array consisting of a set of behavioral scoring elements that are returned to the client environment in real time. This analysis uses intelligence anchors such as IP, email, account, device fingerprint, or device ID to analyze current and historical behavioral interactions across the full NuData network to identify anomalies and solve specific client use cases. The platform also allows clients to return real-time feedback, allowing the NuData models to further learn in real time.
- **Score:** NuData generates a numeric score that provides a risk value for the event profiled. The score is built with data that includes behavioral observations, and deviations from expected behavior. The client decides what level of risk they want to place in each score band depending on their risk tolerance.
- **Real-time evaluation and customization:** NuData has a set of rules built for each use case that are deployed with the platform. The client or NuData can propose to add or modify the rules to customize them further
- **Real-time policy enforcement:** NuData can facilitate real-time policy enforcement through the NuData policy enforcement engine. It can dynamically display interdictions such as an SMS, Push to Mobile, or bot-challenges, among others. Along with providing the full mitigation solution, NuData can intelligently

alert when in-house client interdiction enforcement policies should be triggered.

- **Insights dashboard:** The dashboard gives user-friendly visualization of the state of the client's traffic at any given time. The client can look at specific insights, such as the key bot characteristics from an attack and the main challenge recommendations from the platform during a period of time. This dashboard provides a clear picture clients leverage to assess the health of their traffic. They can also create custom reports and dashboard views.

Customer support for clients

NuData clients have a team supporting their goals that works during the entire relationship. This team includes a data analyst and a customer success expert to help the client reach their business goals with the security platform. Clients from every region benefit from this personalized support, leading **NuData** to be designated the Most Customer-Centric User Validation Solutions Provider by the Technology Innovator Awards.

When clients need an urgent request, the service prioritization follows a three-tier process:

1. **24/7 emergency support:** A 15-minute response SLA, including outages, major performance issues, etc.
2. **Non-production impacting:** A 24-hour response SLA
3. **Customer success manager:** Offered as needed, such as for a long-term strategy
4. **Service levels for availability:** Guaranteed at 99.7 percent, with a 300ms processing time Service Level Agreement (SLA) for all NuDetect API calls

Prior to integration, the Customer Success team is engaged with the client and maintains that support through the growth phase. The key focus centers on the identification of client pain-points, success criteria, product education, and management of the 30-day modeling period to adapt rules and processes to the client's specific traffic and platform.

BehavioSec

The **BehavioSec** platform uses deep authentication to continuously verify user identity with reduced friction across millions of users and billions of transactions. They help organizations with a number of use cases.

Account Takeover

While organizations invest significant resources to insulate from attacks, account takeovers remain a problem. In addition, many costly business challenges like manual fraud analysis and customer attrition from friction can increase costs associated with this approach.

BehavioSec helps manage account takeover (ATO) with **Deep Authentication**, a new method of verification powered by behavioral biometrics. Deep Authentication automatically verifies the human behind the digital identity without adding friction– allowing organizations to keep fraudsters at bay while helping to reduce costs.

New Account Fraud

BehavioSec addresses New Account Fraud with **Population Profiling** powered by Behavioral Biometrics. Using data gleaned from the behavior of a population of normal users, BehavioSec can help you quickly pinpoint fraudsters, whether bot or human.

Checkout Fraud

BehavioSec reduces Checkout Fraud by using **Population Profiling** and **Deep Authentication,** both powered by Behavioral Biometrics. Using metadata from normal behavior and previous customer interactions, BehavioSec can detect fraud without

BehavioSec

At a Glance:

ATO Detection Capabilities

Account/Client Management

Pre-Authorization Functionality

BehavioSec 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.

adding friction. It allows merchants to focus on improving customer experience and conversion rates.

Risk-Based Authentication

BehavioSec offers Risk-Based Authentication through **Deep Authentication**. By verifying users' identities based on how they continuously interact, authentication becomes an ongoing process, not just a one-time step. Best of all, this is done transparently, with no added friction to the customers.

Featurespace

Headquartered in Cambridge, U.K., and Atlanta, U.S., **Featurespace** offers Enterprise Financial Crime prevention for fraud and Anti-Money Laundering. **Featurespace** also offers Adaptive Behavioral Analytics and the new Automated Deep Behavioral Networks (a novel Recurrent Neural Network architecture to create a smart memory, automating the process of feature discovery and fast-tracking data science exploration), both of which are available in the **ARIC™ (Adaptive Real-time Individual Change-identification) Risk Hub**, a real-time machine-learning software that risk-scores events to prevent fraud and financial crime.

Solutions & Functionality

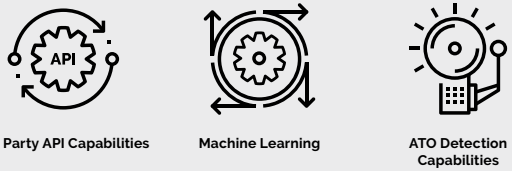
Featurespace's technology attempts to mimic a human-like ability to profile people over time through the **ARIC** platform, which uses their proprietary Adaptive Behavioral Analytics and Automated Deep Behavioral Networks to model and predict real-time individual behavior. This functionality allows computers to understand when an individual customer's behavior is out of character; the platform then automatically evaluates the risk. The technology can be deployed on-premise or via secure cloud, and it is scoring transactions from over 180 countries. In 2018, the **ARIC** platform risk-scored an estimated 15 billion transactions worldwide.

A custom **ARIC** model can be created for every level of potential interaction, from card issuer to acquirer, all the way to the merchant level. Further, an individual context profile is built for every customer, providing additional information for the risk models. If clients manage their own data-science models, the technology allows clients to import these models alongside the **ARIC** platform's own.

FEATURE SPACE

OUTSMART RISK

At a Glance:



3rd Party API Capabilities | Machine Learning | ATO Detection Capabilities

Featurespace 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.

Featurespace

This can be especially helpful as volumes increase. For example, during peak shopping season, the typical rules-based approach often forces institutions to lift rules restrictions, reducing potential review volume to improve scalability during those periods. However, this can allow fraudulent attacks below these increased thresholds. The machine-learning approach taken by **Featurespace** detects anomalies in real time without the requirement of these increased-risk thresholds.

Featurespace has understood customer needs for better payment fraud protection, introducing **ARIC's** tiered, multi-tenancy solution. It provides businesses with a holistic view of their customers and can also protect them with custom industry models and the **ARIC** White Label UI for each customer. **ARIC** is available as a single-tenancy or multi-tenancy solution.

Shape Security

Shape Security protects merchants from increasingly sophisticated automated cyber attacks that employ advanced evasive techniques like Web Application Firewalls (WAFs), Inter Process Communication (IPC), and Distributed Denial of Service (DDoS) tools on web and mobile applications.

They are a real-time adaptive defense platform that protects merchants from most automated level of attacks. They provide 24/7 threat monitoring and incident response. Their products include:

- **ShapeShifter Elements:** A real-time enforcement of security countermeasures to protect web and mobile applications.
- **Shape Mobile SDK:** A framework for mobile apps on iOS, Android, and Windows platforms giving real-time attack deflection on mobile Application Program Interfaces (APIs).
- **Shape Protection Manager:** Provides a cloud-based management of ShapeShifter.

Their primary goal for merchants is to protect against:

- **Account Takeover (ATO):** Defends against this on a larger scale in which fraudsters are using automation to test user names and passwords.
- **Content Scraping:** Uses automation to scrape information for use in another application.
- **Application Denial of Service:** A brute-force automation that overloads a site capacity to the point it breaks.

At a Glance:

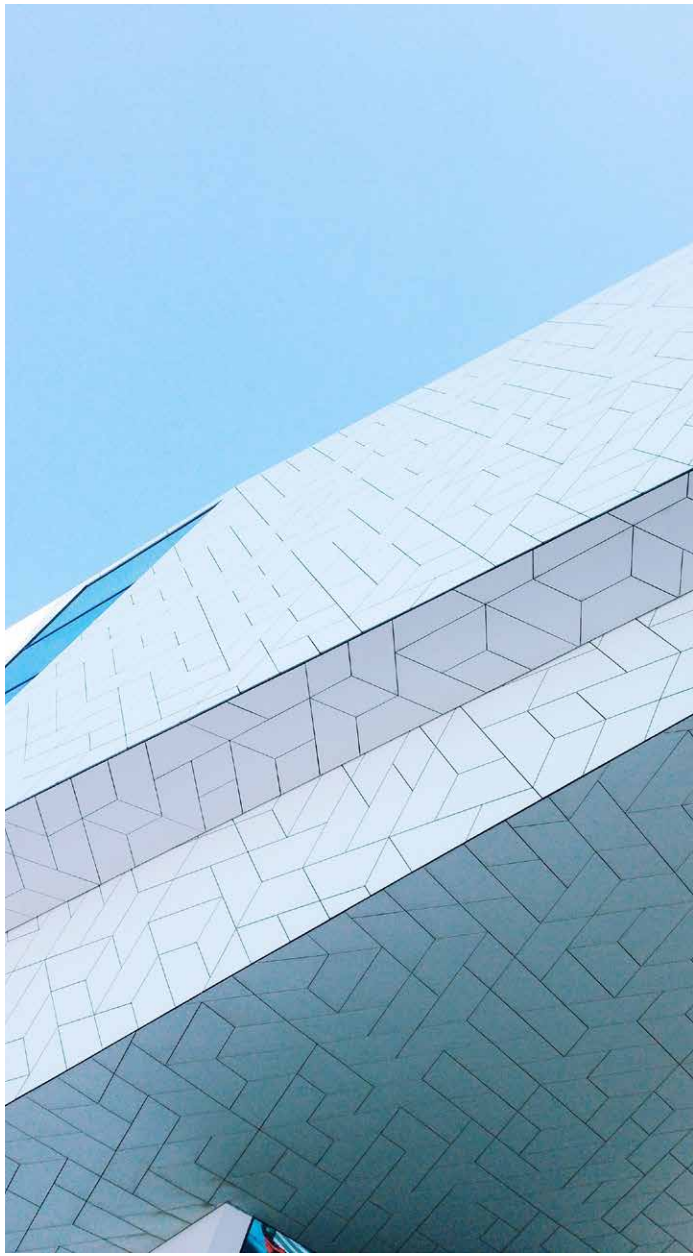
User Behavior Capabilities

Shape Security 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 provides fraud prevention, chargeback management, digital identity, and payment gateway solutions to customers spanning ecommerce, financial services, and other diverse industries worldwide. **Accertify's** layered risk platform, machine-learning backbone, and rich reputational community data makes it possible for clients to address risk pain-points across the entire customer journey—from account creation to authentication, activity monitoring, payment, and disputes.

Accertify' s 3D Secure (3DS) Solution

Accertify's 3DS solution is available as a stand-alone authentication product or as part of their end-to-end authentication management solution. The 3DS solution supports both 3DS 1.0 (3DS1) and EMV 3DS 2.1 (3DS2), with 3DS2.2 launched in early 2021.

3DS protocol enables the card issuer to authenticate the cardholder prior to an authorization being sent, using data supplied within the 3DS message, which can be combined with issuer's own risk solutions to provide frictionless authentication. Alternatively, they can request that the cardholder enter a password or PIN if they feel the payment is risky.

The Frictionless Flow and the Challenge Flow

If the issuer authenticates the cardholder using only the data supplied in the 3DS message, there is no requirement for the cardholder to enter a password or PIN. This is called a frictionless flow. However, if the issuer is concerned about the payment, they can ask the cardholder to enter a password or PIN along with their card data. This data is entered into a separate window at the checkout stage, which is managed by the issuer. The merchant is not able to view either the questions asked, or the responses provided. This is known as a challenge flow.

Accertify
AN AMERICAN EXPRESS COMPANY

At a Glance:

Accertify 3D Secure

Fraud Liability Shift

Once the issuer has authenticated the cardholder, either via a challenge or frictionless flow, the issuer becomes liable for the transaction, should it prove to be fraudulent. This is known as the Fraud Liability Shift (FLS). It is important to note that the FLS policy is set at the scheme level and can be revoked by individual schemes. The third option for the issuer is to decline to authenticate. This option is used in those instances when there is an issue with the card account, or the payment is deemed high risk by the issuer's fraud solution.

Additional Protocols

The frictionless flow, challenge flow, and declined authentication flows as described above have been in place for a number of years. But the infrastructure that supports these flows has evolved considerably over time. The initial version of 3DS, 3DS1, was launched in 1999 by VISA. The 1.0 protocol proved successful in reducing ecommerce fraud, so similar protocols were created by card schemes including American Express and MasterCard.

Most major card schemes developed their own version of 3DS 1.0. However, it was designed to work in a browser-based shopping environment, and thus did not transfer well to mobile app-based shopping. Subsequently in 2016, EMVCo published the specifications for 3DS2. The 3DS2 specifications were written with cross-industry input and provide a standardised solution for all merchants, acquirers, and issuers to follow. 3DS2 is a significant evolution from 3DS1 and the primary enhancements include:

- **Data sharing:** 3DS2 shares ten times as much data as 3DS1. This includes device, session, and IP data. This data enables the issuer to make better decisions when assessing the authentication request.
- **Mobile app optimization:** 3DS2 is designed to work with both a browser and app/device-based shopping experience. For example, 3DS2 can be implemented seamlessly into the merchant app, providing a much more customer-friendly experience.
- **Non-payment based authentication:** 3DS1.0 was limited to payment flows, but 3DS2 supports non-payment flows. For example, 3DS2 can be used to authenticate the provisioning of a card into an e-wallet.
- **Tokenization:** 3DS2 supports tokenized transactions, which helps to reduce the risk of the card number being compromised.
- **Support for a variety of authentication methods:** This includes one-time passcodes, biometrics, and out-of-band authentication.

The enhancements above and a number of additional enhancements are currently available through **Accertify's** 3DS2 solution. **Accertify** is currently working on the next evolution, 3DS2.2, which will provide even more features and functionality.

Accertify 3D Secure

Merchant Fraud Strategy

Accertify believes that 3DS2/2.2 should be an essential part of a merchant's fraud strategy. 3DS2 not only brings financial benefits through fraud reduction and the fraud liability shift, but it can also help to protect merchants' brand by ensuring customers feel secure when making purchases via app or website.

Strong Customer Authentication (SCA)

Furthermore, in Europe, 3DS2 has become the default solution for merchants that need to comply with new regulations, i.e., Strong Customer Authentication (SCA). SCA requires that all intra-European Economic Area (EEA) transactions are authenticated by two of the following three factors:

1. Inherence (e.g., biometric)
2. Possession (e.g., device)
3. Knowledge (e.g., PIN/Password)

The scope of SCA is limited to cards issued within the European Economic Area (EEA), and there are exemptions available. At a minimum, all ecommerce merchants based in the EEA should implement 3DS as part of their compliance strategy in meeting the newly enforced EEA regulation requirements. A merchant's failure to comply with the new EEA regulation may cause a significant number of sales to be declined by the respective card issuers. **Accertify** believes that merchants should not only implement 3DS, but they should also implement an SCA optimisation solution. This enables the merchant to maximise all the available exemptions and scope criteria to ensure as many sales as possible are processed without the potential for friction associated with 3DS. Identifying payments that are out-of-scope or exempt, can help the merchant provide the optimal customer experience.

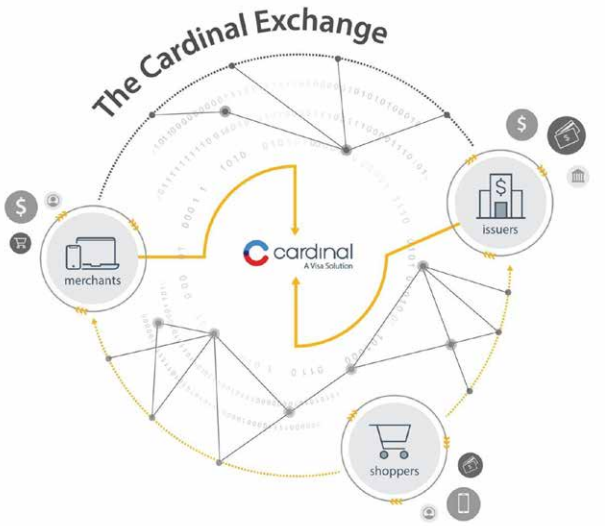
While 3DS1 supports SCA compliance, a stronger combination is to integrate both 3DS1 and 3DS2. 3DS2 is a substantial improvement from 3DS1 and provides the merchant with the ability to share more information about the payment and SCA-related information like exemptions, mandated challenges, etc.

CardinalCommerce

CardinalCommerce is a leading payment authentication provider offering a suite of payment decisioning solutions. **Cardinal's** goal is to make authentication a trusted standard for everyone within the digital commerce ecosystem by offering solutions that provide the data that organizations need when they need it.

Since 1999, **Cardinal** has been offering payment authentication and is an EMVCo member, playing an active role on their business and technical committees.

Cardinal works with merchants and issuers to deliver a trusted, often frictionless experience for everyone in the digital commerce ecosystem. They develop smart solutions and simplify and accelerate authentication for their customers and their customers' customers. Through the **Cardinal Exchange**, they can offer merchants and issuers visibility to both sides of the transaction and access to more actionable data, which can positively impact the decision-making process, Through shared data, merchants may receive benefits like reduced false declines and fraud, increased authorizations, improved customer experience, quicker response times, and more control over step-ups, which can result in more authorizations.



At a Glance:

- 3rd Party API Capabilities
- Pre-Authorization Functionality
- Account/Client Management

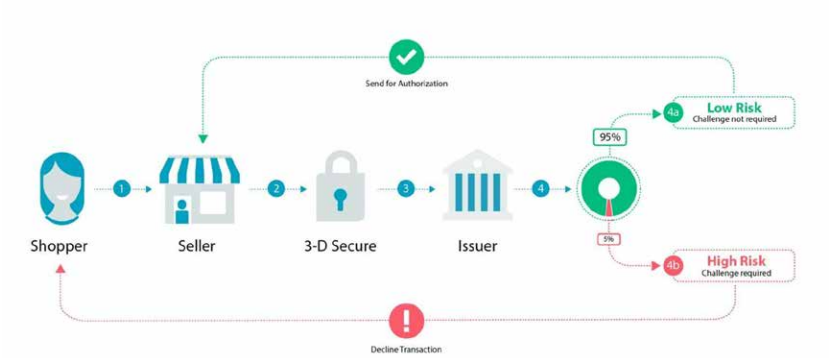
CardinalCommerce

How it works:

Cardinal's EMV® 3-D Secure solution can support both issuers and merchants by providing increased insight into both sides of many transactions (especially in the U.S.). Issuers receive more than 150 data points during EMV 3DS authentication, including device data, transaction data, and merchant data, which is combined with what issuers already know about their own cardholders. Using this data, issuers can make better risk decisions and authenticate most transactions behind the scenes, which can help decrease friction.

When a consumer shops with a digital merchant and the merchant uses Cardinal for authentication, the process begins before checkout and the data is collected while the consumer is browsing.

Graphic 1. The checkout flow



The consumer often does not even realize authentication is happening and the entire process takes place in milliseconds. When a challenge is requested, authentication methods such as one-time passcode (OTP) and biometrics are used to reinforce cardholder protection. As issuers get access to more data on the consumer's transaction request, including device and checkout information, only high-risk transactions should be challenged, unless the transaction is happening in a regulated region where two-factor authentication is required. And this is good news – as EMV 3DS is doing what it is supposed to - helping to stop fraud and lower false declines.

Products:

Cardinal's suite of payment decisioning solutions can help provide better informed decisions and higher approval rates with network agnostic technology.

Merchant products

3-D Secure and authentication solutions:

Cardinal's 3-D Secure solution for merchants is **Cardinal Consumer Authentication (CCA)**, a network and version agnostic 3DS solution designed to help increase approved sales and reduce fraud. It is powered by a global authentication network of tens of thousands of merchants, thousands of issuers, gateways, and acquirers processing billions of transactions a year.

CardinalCommerce

CCA offers a rules engine that allows merchants to create rules from data points collected during the purchase request, offering flexibility in the decision-making process. The CCA rules engine exposes over 150 data points to tailor when, how, and in what way to apply authentication to a merchant's transactions. Ranging from Transaction Amount to Travel Extension fields (such as Departure Airport), merchants have access to data fields that affect their specific customers.

Graphic 2. CCA

Data Only solutions

These solutions can provide a frictionless e-commerce transaction protocol that takes in data sets from the merchant in order to generate and share network trusted intelligence with the issuer to help increase approvals and lower false declines. These solutions are for the many merchants who would prefer a guaranteed frictionless experience over the traditional benefit of liability protection that 3-D Secure offers, and merchants that are focused on trying to maximize approvals and are not hypersensitive to fraud.

In addition, for merchants in unregulated areas, like North America, these Data Only solutions offer the benefits of additional data with minimal latency and no chance of a challenge.

The Cardinal Mobile SDK

The Cardinal Mobile SDK supports merchants' ability to activate 3-D Secure into their checkout flow. **Cardinal's** Mobile SDK, using EMV 3DS, provides a customer-friendly mobile experience. **Cardinal** currently supports Android and iOS (Swift and Objective C) platforms. The EMV 3DS was specifically designed with mobile devices in mind offering auto rendering, landscape support, dark mode support, and UI customization.

Additional features and capabilities:

- **Delegated Authentication:**
  Delegated Authentication is the framework that allows merchants that qualify to perform SCA on behalf of the issuer. In the EU, where SCA is required to be performed for the majority of e-commerce transactions, merchants can implement FIDO authentication within their checkout experience to help issuers meet the regulatory requirements of SCA.
- **FIDO:**
  FIDO is a standardized authentication protocol used to strongly authenticate a cardholder on their device, without relying on passwords or one-time passcodes (OTPs). FIDO can be used with EMV 3DS and Delegated Authentication to provide a solution for

strong authentication, helping to address PSD2's strong customer authentication (SCA) requirements. Unlike password databases, FIDO stores personally identifying information (PII), such as biometric authentication data, locally on the user's device to protect it. FIDO is used to associate an authenticated cardholder and their payment credential(s) to a FIDO-compatible device. The cardholder is bound to their device and payment credentials to provide a faster and more secure checkout in the future.

- **Data Exchange API:**
  Data Exchange API (DX API) was built to give merchants additional data and real-time insights during the transaction process, prior to authentication taking place. This helps merchants have greater visibility into issuer behavior, technical support, and performance, in order to determine the most suitable authentication strategy for their business.
- **The Merchant Portal:**
  The Merchant Portal provides merchants real-time data, including the ability to access specific transaction and authentication data, view error messages and descriptions, and filter, narrow, and organize data how they choose. This enables merchants to easily troubleshoot potential issues and respond to customer inquiries in real time.

Cardinal supports a growing number of major and regional credit and debit card networks. Current certifications include:

- EMV 3DS v2.1: Visa, Mastercard, American Express, Discover, JCB, Union Pay International, ELO (Brazil), Cartes Bancaire (CB) (France). Coming in 2022: ITMX (Thailand), EFTPos (Australia).
- 3DS 1.0: Visa, Mastercard, American Express, Discover, JCB. Note: these networks are set for an October 2022 sunset.
- EMV 3DS v2.2: Visa, Mastercard, American Express, Discover, JCB, Union Pay International

Issuer products:

Cardinal offers a suite of products, features, and capabilities for issuers. Our 3DS solution for issuers is:

- **Visa Consumer Authentication Service (VCAS)**
  VCAS, Cardinal's issuer ACS, uses real-time risk-based assessments across all major card networks, giving issuers the ability to change with the payments landscape. **VCAS** is a data-driven hosted solution designed to support an issuer's authentication strategies with their 3DS program. When a consumer makes a purchase, **VCAS** scores each transaction, enabling improved risk assessment and can support better decision-making. It also gives issuers the ability to create, test, and publish authentication rules within **Cardinal's** portal.

CardinalCommerce

Support for PSD2 SCA:

Cardinal has focused on PSD2 SCA requirements since the initial Regulatory Technical Standards (RTS) were issued by the European Banking Authority (EBA) in 2017

PSD2 SCA related offerings include:

- SCA-compliant methods, including biometrics
- Knowledge-Based Questions and Answers plus One-Time-Passcodes (KBA + OTP)
- For behavioral biometrics, the ability to identify "two legs in" (where both issuer and acquirer are based in the EEA)
- For issuer transactions and exemption application through transaction risk analysis for issuers and acquirers

As issuers integrate these tools, merchant partners are able to improve the consumer authentication experience through compliant SCA methods.

Additional highlights include:

- Works with 7 of the Internet Retailer's Top 10 merchants[1]
- Works with 6 of the top 10 U.S. credit card issuers and 6 of the top 10 U.S. debit card issuers[2]
- Works with over 20 processors that serve issuers and over 100 processors that serve merchants around the globe[3]
- **Cardinal** support network offers in-region local and global support, anchored by **Cardinal's** team of product experts and 24x7x365 online support
- Harnesses insights across Visa's global network of over 3.4B cards to drive better decisioning

[1] Source: 2019 Digital Commerce 360 (Internet Retailer) Top 500, North America, 2019 Edition

[2] Source: Nilson Report, issue 1156, June 2019. Top issuers in U.S. by purchase volume, 2018 (includes credit, debit PIN, debit signature and prepaid cards),

[3] Source: Cardinal FY20 CCA and VCAS Performance Data

Cybersource's 3-D Secure Solution

Cybersource is a wholly owned subsidiary of Visa, Inc. Through global reach, modern capabilities, and commerce insights, **Cybersource** creates flexible, creative commerce solutions for everyday life—experiences that delight customers and spur growth globally. **Cybersource** processes billions of secure transactions every year. Each one provides insights to optimize fraud prevention, capture more revenue, and improve customers' authorization rates. Together with Visa's other subsidiary companies, CardinalCommerce and Verifi, **Cybersource** 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.

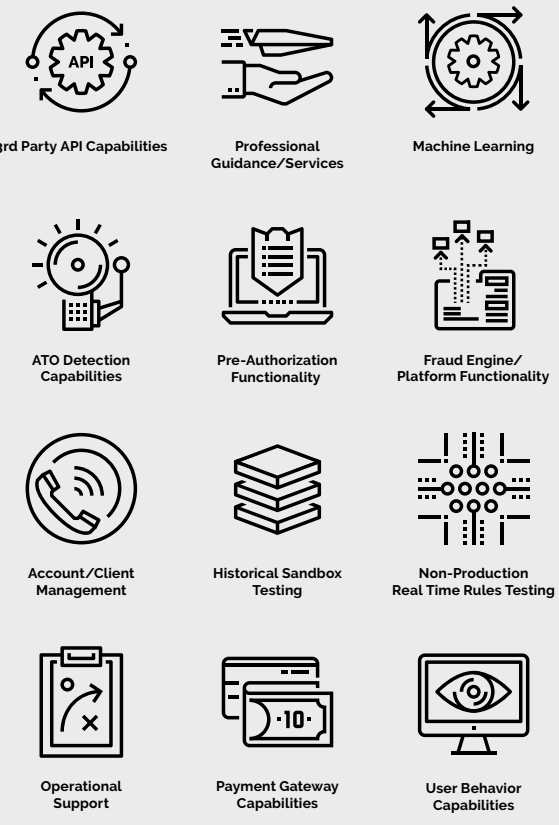
Payer Authentication

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 **Cybersource** Decision Manager helps businesses quickly add Payer Authentication to their **Cybersource** fraud management solution.

cybersource
A Visa Solution

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.

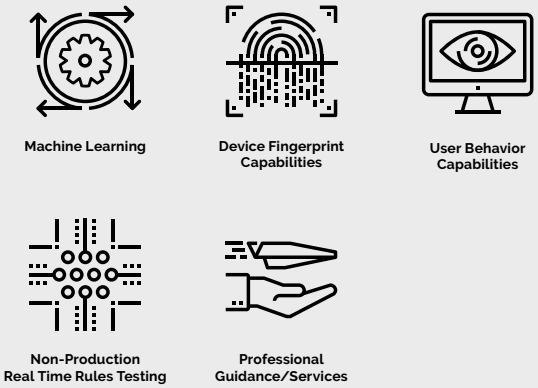
Outseer 3-D Secure helps support Key Performance Indicators (KPIs), including:

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

In the first half of 2021, **Outseer 3-D Secure** protected more than $100 billion in payment volume.

OUTSEER
An RSA Company

At a Glance:



Outseer 3-D Secure™

Products, Solutions and Technologies:

Outseer 3-D Secure is an Access Control Server (ACS) that specializes in protecting any 3-D Secure transactions coming from supported channels, including: mobile apps, mobile browsers, web browsers, or IoT devices. **Outseer 3-D Secure** can be used by Financial Institutions, specifically those that issue credit or debit cards and fintech companies that offer advanced digital payments options.

Two key differentiating aspects of the **Outseer 3-D Secure** solution are the **Outseer Risk Engine™** and the **Outseer Global Data Network™**:

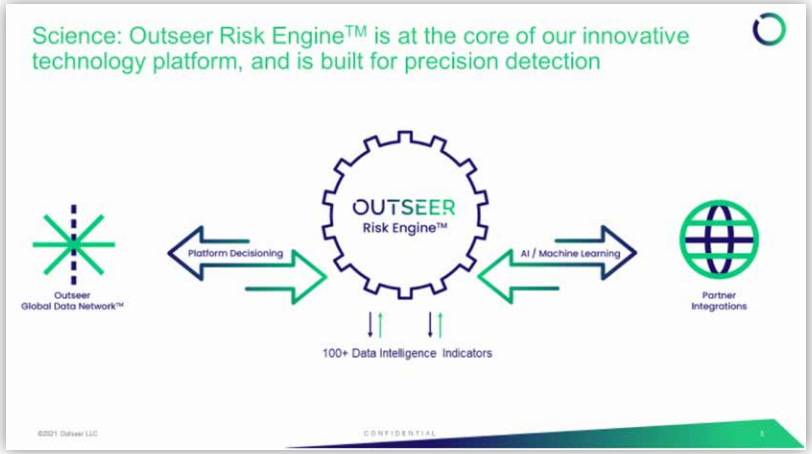


Diagram 2: **Outseer Risk Engine™**

- With the Outseer Risk Engine™ at its core, Outseer 3-D Secure evaluates each transaction in real time to determine the probability of transactions being fraudulent or genuine.

The **Outseer Risk Engine** analyzes more than 100 different fraud indicators to evaluate the risk of a transaction in real time and produce a risk score. The score is based on device and behavioral profiling data elements from the 3-D Secure protocol, along with intelligence from the **Outseer Global Data Network**. The risk engine combines data inputs, machine learning, and case management feedback to provide accurate risk evaluations to mitigate fraud.

All available factors are taken into consideration, but weighed according to relevance, so that the most predictive factors contribute more heavily to the score. The predictive weighting calculations are updated daily based on the feedback from case management, chargeback data, and authentication results.

Within the **Outseer 3-D Secure** product, the **Outseer Risk Engine** efficiently learns to provide a fully tuned risk calculation based upon the customer's specific use cases and implementation. During the initial learning period, the **Outseer Risk Engine** takes into account a number of factors and provides customers the option to tailor inputs, business rules and other implementation considerations. This allows customers to evaluate in "test mode" to

Outseer 3-D Secure™

understand the impact of different rules and conditions prior to being deployed in production.

- The **Outseer Global Data Network** is among the first contributory data consortiums for fraud prevention that amasses risk signals from across thousands of **Outseer** customers and partners worldwide. When a member of the network marks an activity as "Confirmed Fraud" or "Confirmed Genuine," the associated data elements are shared across the network. When an activity is attempted and includes one of the elements from the **Outseer Global Data Network**, the risk is automatically adjusted.

Step-up Authentication:
Step-up authentication is reserved for a subset of transactions that truly warrant closer scrutiny based on higher risk and/or defined policies. **Outseer 3-D Secure** offers out-of-the-box step-up authentication options as well as a flexible interface to integrate with an organization's own authentication methods.

Reporting and Analytics:
Outseer analytics application provides **Outseer 3-D Secure** customers with full visibility into their 3-D Secure transaction data. The analytics application makes daily and monthly monitoring metrics, fraud detection rates, and rule performance data available so customers can align their respective solutions with their risk tolerance levels and business priorities.

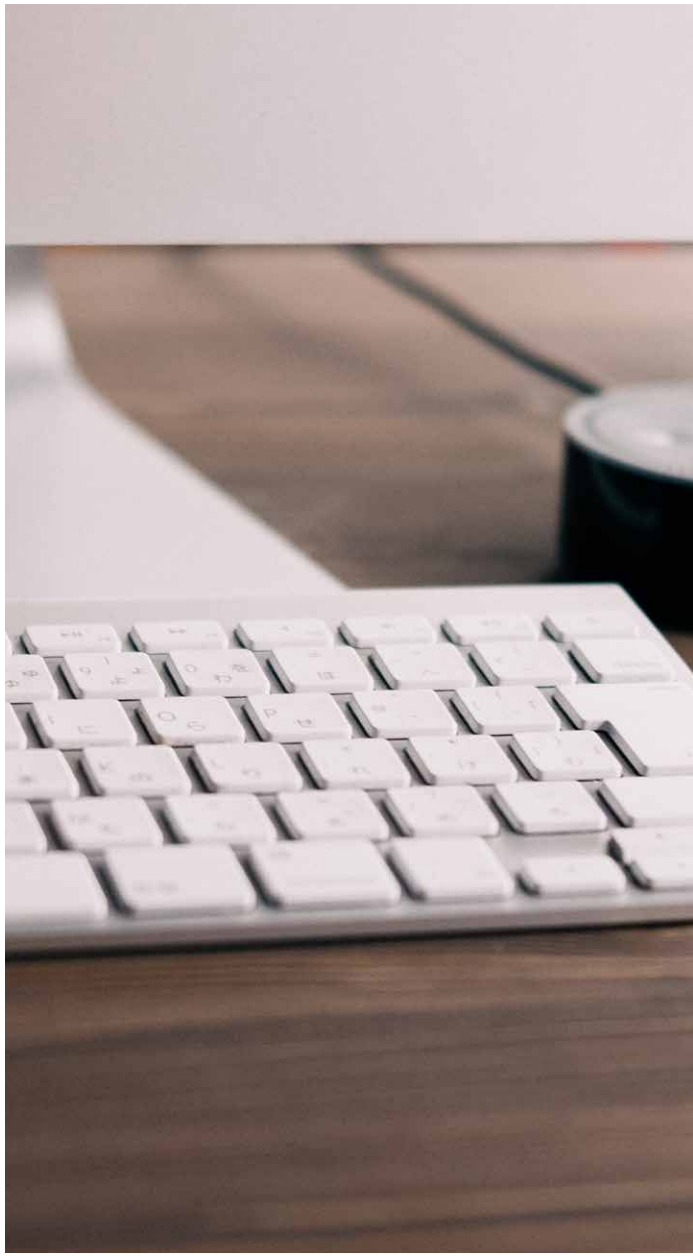
The dashboard is populated with reports that allow customers to:

- Visualize and highlight trends and outliers
- Evaluate different views of the data and drill down into granular details
- Make near real-time changes via a flexible and dynamic interface

For more information regarding the full portfolio of **Outseer** products and solutions, see pages 79-82

Device Identification, Recognition & Reputation

Solution providers in this category focus on risk factors of the device itself. By considering context, behavior, and reputation, merchants can determine where the device is really located, what a device has been up to, and the history of fraud associated with the device.



ThreatMetrix

The ThreatMetrix platform supports universal fraud and authentication decisioning, built on a repository of **Digital Identity Intelligence**, which is crowdsourced across its 5,000+ global clients. (And as of this report's publishing, the company is being purchased by RELX Group and will become part of its LexisNexis Risk Solution division.)

ThreatMetrix ID is the technology powering **Digital Identity Intelligence**, helping businesses elevate fraud and authentication decisions from a device to a user level and unite offline behavior with online intelligence. **ThreatMetrix ID** helps businesses go beyond device identification by connecting the dots between the myriad pieces of information a user creates as they transact online. It then looks at the relationships between these pieces of information at a global level and across channels/touchpoints.

This intelligence is operationalized using the **Dynamic Decision Platform**, which incorporates behavioral analytics, machine learning, case management, and integration capabilities to help businesses make the best trust decisions across the entire customer journey. In tandem, **ThreatMetrix Smart Authentication** provides a framework that incorporates risk-based authentication (RBA) with Strong Customer Authentication (SCA) that provides an approach to protecting customer accounts while minimizing friction for trusted users.

ThreatMetrix

At a Glance:

Device Fingerprint 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.

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 provides fraud prevention, chargeback management, digital identity, and payment gateway solutions to customers spanning ecommerce, financial services, and other diverse industries worldwide. **Accertify's** layered risk platform, machine-learning backbone, and rich reputational community data enables clients to address risk pain-points across the entire customer journey—from account creation to authentication, activity monitoring, payment, and disputes.

Solutions and Functionality

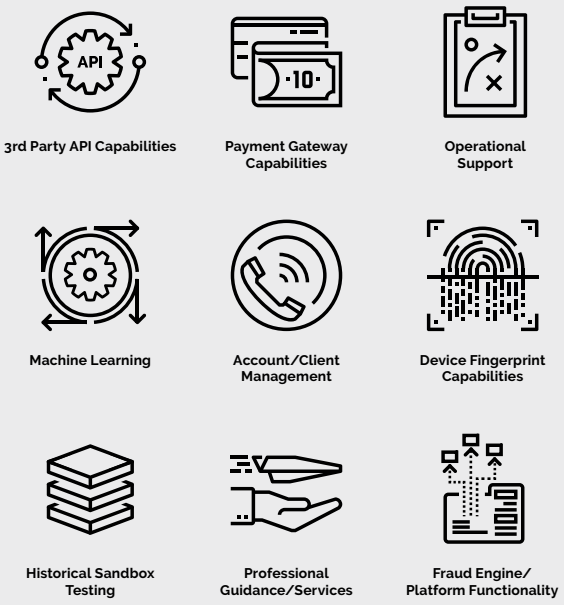
The **Accertify** Interceptas® Platform is a software-as-a-service offering that allows clients to adapt their fraud-screening strategy in real time. It utilizes machine learning models, configurable fraud and policy rules, and robust reputational community data. The platform can perform risk assessments in real time, in batches, or via manual review, and offers a wide variety of pre-integrated connections to third party data providers. The platform is PCI-DSS Level 1 certified and is SOC2 and ISO 27001 compliant.

Accertify's Interceptas® Platform includes core functionalities such as:

Scoring Functionality: At its core, the Interceptas® 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 near-infinite range of policy checks to live alongside their fraud screening strategy. The user-friendly interface is designed to allow non-IT resources to author rules and make comparisons to adjust risk assessment. The same functionality can conditionally invoke API calls to third parties or leverage **Accertify's** rich sources of community data.

Accertify
AN AMERICAN EXPRESS COMPANY

At a Glance:



Accertify, Inc.

Case Management: The Interceptas® Platform offers clients a configurable tool that can be used to analyze data, assess risk, and report and manage fraud risk screening. While the majority of traffic is handled via a machine-learning and rules-based approach, the case management system allows clients to build workflows that suit their team structures and support their SLAs.

In 2022, Accertify's Case Management changes will focus on a few key themes, including:

- Strengthening their cross-client fingerprint and deploying their next generation, machine-learning powered browser fingerprinting capability, focused on complex fingerprint challenges such as corporate networks, aggregators, and mobile browsers
- Expanding user behavioral analytic (UBA) capabilities in native mobile apps, simplifying integration with support for popular mobile app development frameworks, and enhancing models and data processing for both browser and mobile
- Expansion of their FIDO-certified solution into native mobile SDKs
- Continued investment in models to expand coverage to a wider variety of account-centric attacks. Examples include bot attacks, account takeovers, promotional abuse, fraudulent account opening, withdrawals, deposits and marketplace transactions.
- Additional capabilities to prevent growing post-fulfillment abuses, like refund and returns fraud
- New features in their case management for bundling transactions into cases, new reports, and more streamlined ways of managing user permissions
- Expansion of fraud liability shift (chargeback guarantee) capabilities

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

- Identification of consistency versus change across transaction elements to reveal threats as they emerge
- Dynamic updates to key data features as the risk grows or diminishes
- Targeted use of community intelligence to bring additional knowledge to clients' transaction decisioning outside of their business interactions

Device Intelligence: Accertify analyzes devices and associated identities transacting across digital channels via mobile applications (InMobile) and mobile and desktop browsers (InBrowser). **Accertify's** device intelligence platform helps clients verify identity, assess and mitigate risk in real time, and optimize the customer experience.

Accertify, Inc.

InMobile provides a Software Development Kit (SDK) that 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:** InMobile analyses connected devices to detect known malicious applications as well as criminal tools, such as location spoofing and IP address proxy apps. Malware files are dynamically updated without client interaction.
- **Rooted/Jailbroken detection:** InMobile protects against increasing—and increasingly complex—rooting methods used by fraudsters, such as Cloaked Root, through Advanced Root and Jailbreak Detection.
- **Trusted Path:** InMobile's security architecture prevents interceptions by providing a complete secure path to transport sensitive information, which is encrypted end-to-end, signed, and digitally protected against replay attacks. InMobile uses Trusted Path to securely communicate sensitive messages.
- **Secure messaging:** Secure means of delivering contextual Two-Factor Authentication (2FA) messages to a registered device through the InMobile SDK and secure Trusted Path that cannot be read by any other device, intercepted, or replayed. This can be a stand-alone offering.

InBrowser provides JavaScript collectors that 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. Collector code can be invoked upon page visit or tied to specific actions, such as Form Submit, based on technical and business requirements. Examples of pages where data collection is typically enabled include account open page, login page, account change/update page, and checkout/payment page.

- Our 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.

User Behavior Analytics (UBA): Accertify offers their clients the ability to track the behavior of their customers' web traffic 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 can provide risk ratings and includes visual representations of a user's journey through a website, including

measurements of page duration, mouse movement, keystroke dynamics, and pasting or auto-filling data into forms.

Link Search Capabilities: Accertify's enhanced link search functionality gives clients the ability to search for historic linkages that can clarify whether an event is out of pattern, or in fact 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.

Rules/Conditions Testing: Clients can test and simulate a condition or conditions using the Accertify rule 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 wouldn't affect the outcome. Production testing gives clients the ability to run transactions through "real-world" conditions such as velocity and negative files.

Profile Builder: Profile Builder helps identify real-time patterns and trends through the dynamic summarization and aggregation of data. Gain insight in real-time 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. No longer is it necessary to anticipate potential risk, wait overnight for a model or algorithm to be updated or calibrated, or have static, stale rules. 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. This eases manual review rates and enables a more efficient and flexible strategy to mitigate risk.

Chargeback Management: Please see full write-up in the **Accertify** Chargeback section of the Paladin Vendor Report.

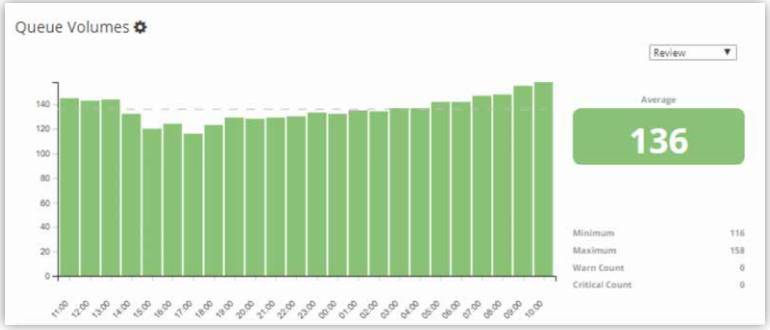
Payment Gateway: This complementary product is for clients seeking a singular platform for payments and fraud. The **Accertify** Payment Gateway is processor-agnostic, giving merchants the flexibility to select different processors for different payment types, and it provides easy connectivity to multiple acquirers globally.

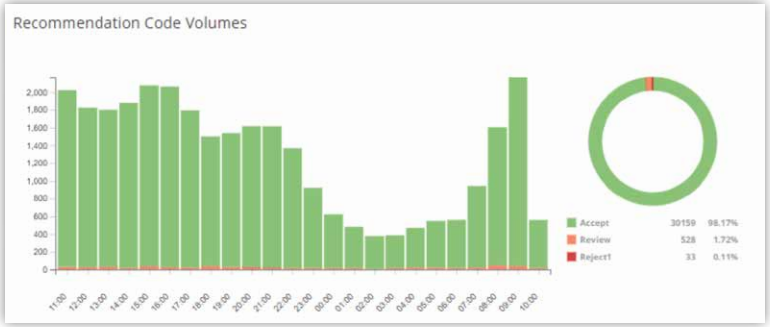
Accertify, Inc.

Reporting:

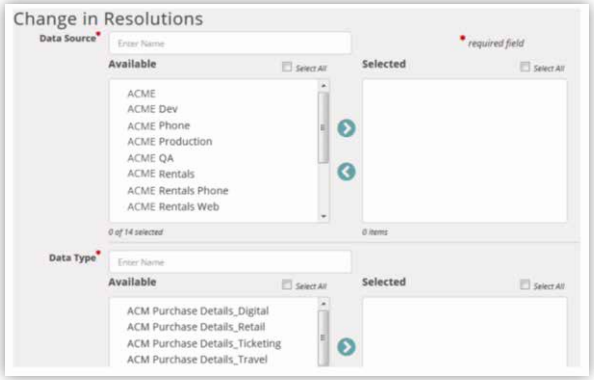
Accertify offers three types of reports:

- **A landing page dashboard:** These are "heartbeat" views of platform statistics—both fraud and chargebacks and performance—individually and across the team.

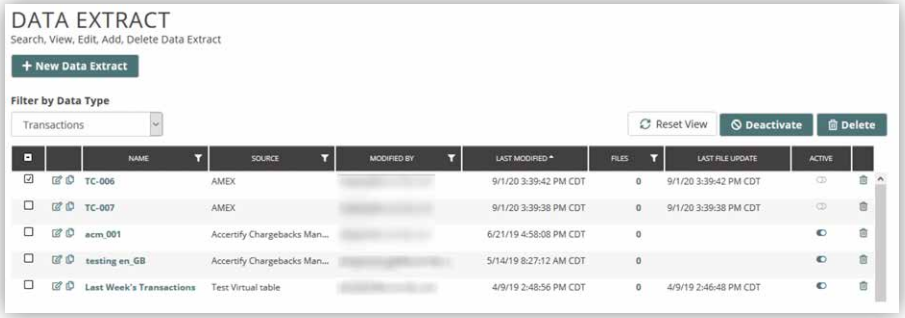




- **Enterprise Reports:** These allow a client to input criteria parameters to specifically drill down and show different types of performance. Examples include monetary metrics, chargebacks, analyst decisioning, rules performance, and more.



- **Data Extract Utility:** This reporting suite allows clients to create either one-time or recurring scheduled reports where they can extract large amounts of data. Reports that are generated via the 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.

Refund Abuse

Accertify recognizes the growing problem of refund abuse and has developed a specific module for merchants struggling to distinguish between legitimate and fraudulent claims.

The Refunds Module from **Accertify** is designed to identify and stop patterns of claims abuse. It allows merchants to accurately discern whether a refund claim is legitimate or fraudulent and how to take the appropriate action. The solution directly addresses the problem without causing unnecessary friction for trusted shoppers. It was developed by working with marquee merchant customers who were having problems with refund abuse.

The Refunds Module is a targeted solution designed to identify and stop patterns of claims abuse, while minimizing friction to trusted customers. Through an easy-to-implement API, this dynamic, risk-based approach allows clients to accurately discern whether a refund claim is legitimate or fraudulent and take the appropriate action. By introducing a standard, risk-based technology approach that considers many different variables, merchants can now effectively begin to measure and monitor a previously undefined process.

The solution uses a combination of machine learning, behavior analytics, and device intelligence to determine the location of the device requesting a refund, whether it is the same location as where the initial purchase was made, and whether it is a human or a bot. The solution can also detect velocity patterns to see when one device is making several refund requests, for example.

Due to the COVID pandemic, many merchants are struggling with an increased volume of returns and refund requests. This has opened a new channel for cybercriminals to exploit as they can fraudulently claim their delivery was not received and request either a re-shipment or a refund.

Merchants also report a growing issue of people returning items that are different from what they originally purchased—such as clothes worn once and returned, or a less-expensive item being returned instead of a more expensive one purchased, or even people returning empty boxes.

Returning the wrong item, or even no item at all, is an operational issue and involves the warehouse teams that receive the package. It is imperative they are communicating with the other teams across the organization when this happens. Merchants sometimes struggle to know if a refund provided was truly fraudulent.

Accertify, Inc.

Services Offered:

Decision Sciences: Accertify's global team of machine-learning experts and data scientists focuses on three core areas:

- Build industry-leading machine learning models, backed by **Accertify's** unparalleled network of reputational community data, to provide clear, defensible reason codes that detail insight into the factors driving the model decision
- Client consultation, including listening to clients' needs, sharing insights, and designing a set of machine learning based solutions to address their needs
- Research and development in pioneering new machine learning techniques, analyzing new data streams, and other activities to provide clients with new data insights and predictive risk behaviors

Client Success Management (CSM): The global team of Client Success Managers are responsible for assisting each client in achieving their fraud and chargeback goals. The Client Success Team is primarily composed of former Directors and Managers of Fraud 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 and work with their client base to assist with adoption of these features and functionalities within their environment to achieve the maximum benefit. **Accertify** Client Success Managers are the conduit into their entire organization, standing by each client's side to guide, grow, advise, and service them as they navigate the complex world of fraud and chargebacks.

Managed Services: Their Managed Services team provides direct operational management of a client's fraud and/or chargeback processes through the Interceptas platform. The team becomes an extension of the organization by providing experienced and comprehensive consultation, geographical coverage, and SLA management.

Support Services: The global Support team employs a "follow-the-sun" approach to deliver 24x7 coverage. By completing rigorous platform and technology training, multi-lingual 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. This library includes best practices, how-to configuration guides, platform documentation, release notes, and more.

Accertify, Inc.

Professional Services: Accertify offers a wide range of professional services designed to help clients optimize fraud prevention, chargeback management, and payments performance. Their Professional Services team are the subject matter experts of the platform. They each bring years of industry expertise and know-how as former fraud and chargeback managers, Certified Fraud Examiners, online technology experts, statisticians, and professional trainers.

ACI Worldwide (ACI Fraud Management)

ACI Worldwide delivers a fully outsourced real-time orchestration payment and fraud solutions which delivers market exceeding acceptance and chargeback rates, with chargeback guarantee and indemnification delivering lowest friction and operational cost for all payment methods, channels, delivery methods, sectors, devices, and globally for Merchants and Intermediaries. Independent of any bank or financial institution, **ACI** helps Merchants increase revenue through flexibility, choice, highest levels of payment conversions, and reduce compliance complexities and losses from fraud.

ACI is committed to innovation and continuous solution enhancement through significant investment in research and development. This ensures that the company's technology, services, and advice continue to provide demonstrable benefits to its customer base of over 80,000 merchants, whether they're served directly or through Intermediaries or Payment Service Providers (PSPs). In 2021, **ACI** received a full patent on incremental learning technology—an industry-first approach to machine learning designed to considerably enhance fraud detection.

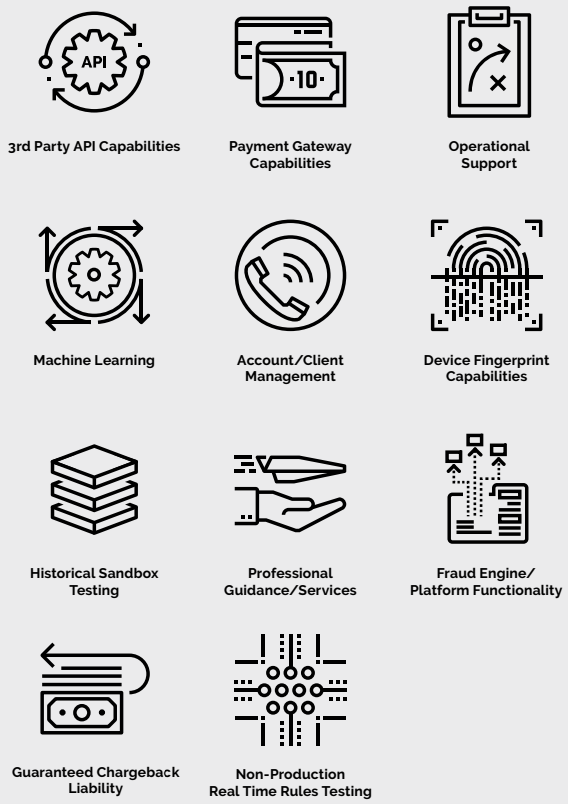
ACI Omni-Commerce platform

ACI Omni-Commerce provides end-to-end payments and risk management services to in-store merchants and card-not-present ecommerce merchants across a variety of verticals, including telecommunications providers, retail, grocery, gaming and entertainment, digital goods, travel and hospitality, fuel and convenience stores, and PSPs.

Within **ACI Omni-Commerce**, the **ACI Secure Ecommerce** solution includes a global ecommerce payments gateway, and a robust, multilayered ecommerce

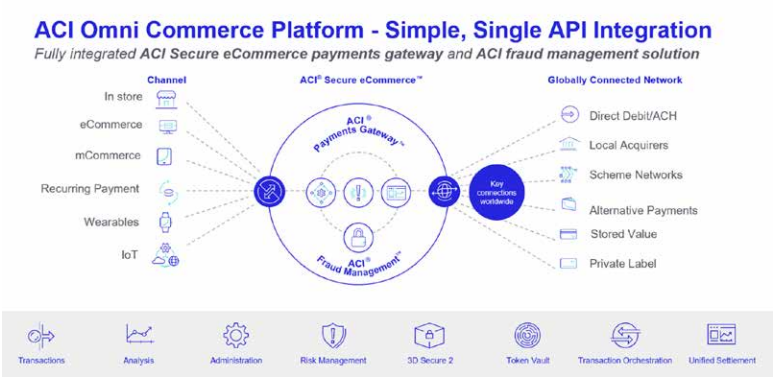
ACI Worldwide
Real-Time Payments

At a Glance:



ACI Worldwide (ACI Fraud Management)

and m-commerce fraud management functionality.



ACI Secure Ecommerce serves as an independent, acquirer-agnostic "one-stop shop" letting merchants manage just one relationship to secure an independent payments gateway with fully integrated ACI Fraud Management offering . This enables customers to choose from a multitude of acquirers and alternative payment offerings through a single API connection. Merchants and PSPs can remain in control of their acquiring and alternative payment relationships and associated commercials, all without having to establish and manage multiple relationships to fulfill their payments processing needs. (Additional details related to the payment gateway can be found via the Paladin Payment Vendor Report.)

As part of **Secure Ecommerce, ACI** offers a sophisticated **ACI Fraud Management** solution.

ACI Fraud Management is a highly customizable, real-time ecommerce fraud prevention solution designed to maximize business growth. The multilayered fraud prevention solution is fully integrated into the payment flow enabling both pre- and post-auth screening and flexible strategies across channels, via the same single API. This, along with high performance metrics and active/active architecture, gives the customer the scalability and flexibility to "sell more and lose less," focusing specifically on achieving:

- **Increased checkout conversion rates,** resulting in additional revenue with no negative impact on false positives, fraud rates, or chargebacks
- **Payments orchestration** providing payment acceptance to over250+ different acquirers and APMs including all major international and domestic card schemes, BNPL (Buy Now Pay Later) solutions, crypto currency payments, online banking solutions, mobile app payments on iOS and Android platforms, and digital wallets
- **Fraud strategies** that are customizable by country, region, channel, payment type, and product type
- **Reduced operational costs** due to the availability of experts who perform payment optimization analysis and offer advice to ensure costs of fraud management remain optimized

ACI Worldwide (ACI Fraud Management)

- **Chargeback Indemnification** aka Guaranteed: Eliminates cost of fraud chargebacks which are approved by ACI and including incentives on approval rates, for a fully managed service offering.
- **Reduced false-positive rates** thanks to multiple tools and technologies ensuring they're kept to a minimum

While the fraud management capability is fully integrated with the **ACI** Secure eCommerce Gateway, it can also be offered as a standalone solution for merchants who only need fraud prevention. **ACI Fraud Management** can also be integrated via one of the company's many intermediary partners, including PSPs, acquirers, marketplaces, and systems integrators.

The **ACI Fraud Management** solution has been through a period of significant transformation in the past three years. The focus has been on building out infrastructure and technical foundations to meet the ever-expanding demands of consumers—and to support merchant needs for scale, choice, flexibility, and security. Investments have delivered increased scalability, enhanced stability, and a centralized "big data" repository underpinned by a sophisticated array of performance-enhancing applications to support data-mining capabilities

ACI has also developed new risk analytics tools within its **ACI Fraud Management** offering, including a Business Intelligence platform and enhanced machine-learning model options.

ACI Fraud Management: A multilayered solution in detail

There is no silver bullet to mitigate fraud and achieve high conversion rates while keeping chargebacks in check. This is why **ACI** deploys a multilayered approach, combining multiple tools and technologies, automation, and human intervention to manage fraud while focusing on conversion. An essential part of the solution uses machine learning and profiling combined with a series of real-time alerts and dashboards. However, other features are also critical to the success of the KPI results consistently. They give merchants flexibility and control over their strategy, with support from a strong team of expert risk analysts and data scientists. Fraud strategies can be modeled to the requirements of each customer and adjusted in real time.

Machine learning

ACI supports and develops multiple machine-learning model options including custom models, merchant-specific models (for

ACI Worldwide (ACI Fraud Management)

larger merchants), and over 15 vertical-focused models (including telco, travel, retail, gaming, and digital). Over 7,000 features are used to create **ACI** models, ensuring high performance regardless of sector. In 2021, **ACI** received full approval on its application to patent the incremental learning technology—an industry-first approach to machine learning designed to considerably enhance fraud detection.

ACI's incremental learning algorithm allows machine learning models to adjust to new behaviors without the need to re-learn everything they already know. This means that new data can be input on a daily basis and new behaviors can be identified in near real-time. Machine learning model performance lasts for longer without degradation and reduces the need for often costly model refreshes. Models are supported by a dedicated team of data scientists. With **ACI's** consortium of shared fraud intelligence data, every merchant reaps the benefit of models that have been trained on high volumes of industry-specific data that are added to daily. This ensures continued consistent and reliable performance.

Profiling

By analyzing the history of transactional data across all **ACI** merchants, positive profiling can match over 100 different data points such as device ID, IP address, email, shipping address, and a wealth of other identifiers. It can even highlight when new variables arise that could affect the risk score. The power of positive profiling lies in the combination of sophisticated analytics with cross-sector merchant consortium data, machine learning, and flexible fraud prevention tools. Positive and negative profiling calculations make fraud event detection and prevention more accurate, and they vastly reduce false positives, which means converting (accepting) more transactions the first time.

- **Link analysis:** Identifies data points associated with a confirmed fraudulent data point, allowing visibility into patterns of emerging fraudulent behavior.
- **Autopilot:** Monitors real-time responses and automatically blocks associated order elements based on high-efficiency strategies or features for a specific period.
- **Auto-Analyst:** This allows further automated investigation outside of the real-time decisioning window. The auto-analyst function is a useful additional layer in the strategy and can be enabled to scale rapidly and in response to increasing volumes when fraud review teams may be under pressure. Auto-analyst can also be used to fast-track time-sensitive transactions such as "same-day" or "next-day" delivery or "buy now / pick up in store" orders.
- **Third-party orchestration:** One integration and one contract with **ACI** gives merchants access to several third-party providers

ACI Worldwide (ACI Fraud Management)

and call the service based on configurable data points in both real-time or near real-time processing steps or decision flows.

  - To manage costs, **ACI** utilizes smart routing functionality so transactions can be qualified in or out for third-party callouts. **ACI** can automate connectivity and receive responses in real time and post real-time to incorporate into the overall core strategy and influence final decisions.

- **Silent mode for strategy testing:** This can be applied to run in parallel through silent mode for a period before applying to active mode (production), such as in champion/challenger strategies. This allows merchants to test the effectiveness of a strategy and optimize it without impacting live customer transactions.
- **Enhanced response:** Additional information is provided, such as the reason for the response given alongside the elements contributing to the result. This can be incorporated into a merchant's (or partner/PSP's) own user interface and internal platforms.
- **Fuzzy matching pattern recognition:** This functionality helps identify linked fraudulent attempts in which address concatenation/manipulation and/or email tumbling might appear as unique transactions to most automated systems. This makes it easier to identify fraud trends and enables fast mitigation action.

Administrative tools

- **Control Center:** A single-sign-on interface provides access to the customer service interface, for strategy and case management and Business Intelligence tool.
  - **Decisioning rationale** on individual transactions, including order data points, responses, Model and Strategy decision explanation in visually appealing detail.
- **Business intelligence (BI):** dashboard and reporting tool provides visibility into KPI Performance, trend analysis, model performance, and chargeback settlement detail, including two years of history. The tool continuously and automatically tracks and labels KPI performance on decision, false positives, chargeback, decline, bank, authentication, and approval rates, etc. It can help identify new and emerging high-risk trends as well opportunities for increased acceptance rates. The tool also allows users to develop, test, deploy, and monitor strategies in active or passive/silent mode. Merchants can view fraud KPIs such as accept, challenge, and deny rates, plus trends on a global and channel basis.
  - **Self service reporting:** This gives clients the ability to build their own reports.
- **Strategy Manager:** allowing merchants to add, delete, and modify overall strategy, which is highly flexible and customizable with several different decision or weighted scoring responses. With an easy ability to reference lists, features, or active sets.

ACI Worldwide (ACI Fraud Management)

Additionally, includes template strategies for ease and speed.

- **List manager:** Enables merchants to create lists that can be referenced within the strategy, such as return abusers or known VIP consumers. The feature can be used for either positive or negative lists.
- **Feature manager:** Create multidimensional features (sophisticated sets of data calculations instructions incorporating several data points, conditions, and chargeback history, or positive history) When coupled with the strategy and list manager, merchants can use the feature manager to create customized conditions, features, and lists to significantly enhance "allow" decisioning for good customer acceptance and to further minimize false positives.
- **Block manager:** Merchants can create positive or negative future decisions any data point sent as part of the transaction.

- **Case manager:** A workflow management tool that allows prioritization of workflows (such as order value and delivery channel).

Expert consultancy

- **Strategy and Payment Optimization Specialist: ACI's** global team of dedicated **team of specialist's** are an inclusive part of the **ACI Fraud Management** service. Analysts cover four continents (and 15 languages) and have access to global payments intelligence and local market knowledge. They have an average of five years of experience, and many are certified ecommerce fraud professionals. All have degrees in math, computer science, or data science. At the start of an engagement, risk analysts collect in-depth merchant background information including historical fraud data. They review existing processes and operations and identify a potential strategic approach.
- **Data Scientists: ACI's** dedicated team of highly skilled data scientists bring decades of experience to the table, and are all educated to MSc and PhD level. The team is responsible for both AI and machine-learning strategies across **ACI's** portfolio. They have over 15 consortium models in production, covering all main verticals from retail to clothing, gaming, and travel. The team continues to innovate, bringing new technology to market, preventing fraud, and helping customers utilize machine learning in a meaningful way. The team is multilingual, with representation in the US and Europe. Academically, the team is well published, with over 30 publications between them, continuing to contribute to the ever-evolving domain of data science.
- **HELP24 Support:** Support can be reached 24 hours a day, seven days a week, 365 days a year, to answer product questions and resolve technical support issues.
- **Manual order review:** Merchants are provided a team of Analysts to validate and authenticate challenged transactions

ACI Worldwide (ACI Fraud Management)

for a final decision of Approve or Cancel. Decisioning accuracy is tracked and monitored to ensure key performance indicators are met, averaging a 99.99% rate. Service can be deployed during season peak periods, weekends, or daily.

- **Chargeback Defense:** An ACI-outsourced process for chargeback and dispute management. Merchants can utilize the service to manage all chargeback disputes, including collation and submission of evidence to support the dispute application.

Integration Process

ACI offers merchants a cloud-based deployment for its ecommerce fraud capabilities.

Integration can range from a couple of days to a couple of weeks, depending on the size of the implementation. It can be accomplished with a simple API integration.

The primary point of contact during integration includes a Project Manager and a Service Delivery Manager who are responsible for guiding the integration process and overseeing tasks like tracking issues, identifying friction points in the process, and coordinating the fraud strategy with the Risk Analyst. The Risk Analyst will begin to develop the initial strategy by analyzing an historical data submission from the client (if available) using at least six months of data of all transactions, followed by a three-week analysis period while coding takes place. The risk strategies will continue to evolve and be refined at regular intervals in conjunction with the merchant to maximize optimization.

In development over the next 12 months

ACI delivered its patented incremental machine-learning capability, which allows for fully automated incremental learning models, removing the need for expensive and time-consuming model refreshes and allow faster new model deployment. 2022 will see machine-learning scoring visualization will also be enhanced.

Other enhancements will include:

- **Weighted scoring:** The ability to provide weighted scoring and prioritization to the multi-layered components within the fraud strategy. By individually weighing the priority of scores, e.g. ranking the importance of specific checks, strategy and validations over others, ensure that acceptance rates are optimized but costly false positives and fraud minimized. The cumulative weighted scores can then be totaled and will ultimately determine the outcome of the overall automated decision. Scores and weightings are regularly reviewed and can be amended as required to ensure optimization. **ACIs** team of Data Scientists and payment optimization specialists will work with the client to agree on weighting plans. This new approach

allows clients to determine how much the model influences the overall decision, allowing for an ML first approach or a hybrid one depending on customer preference.

- **Decision intelligence: ACI** is now able to provide automated strategy enhancement recommendations. Using **ACI** established Artificial intelligence, we have developed Decision Intelligence to automatically inform customers of recommended changes to the strategy to ensure continued optimization and performance. In addition, the recommendations come with justification stats to show the results on performance based on historical data and trends, which customers can review before accepting recommendations that auto-apply the changes to their strategy – this ensures continued optimization of the strategy. Customers can decline recommendations and continue to make manual amends if required or accept changes and manually adjust as needed (e.g. in the event of flash sales or offers), ensuring flexibility and control over the strategy.
- **Graphical link analysis:** To discover connections between different customers, identifying criminal or suspicious activities that uncover how fraud rings operate—and allowing for a continuous and efficient way of blocking organized fraudulent activities.

ClearSale

ClearSale provides a complete, data-science-backed fraud solution that prevents 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 A.I. technology and expert manual reviews to help maximize a business's revenue, approve as many valid orders as possible, and keep customers happy.

Proven Protection

ClearSale was the first full outsourced fraud management solution on the market in 2001 and the first to offer chargeback guarantees. ClearSale remains the largest and only solution with the scale, flexibility, expertise and experience to support any merchant globally.

1500+	5000+	20+	160+	99%
Specialized Analysts	Clients Worldwide	Years of Experience	Countries	Customer Retention Rate

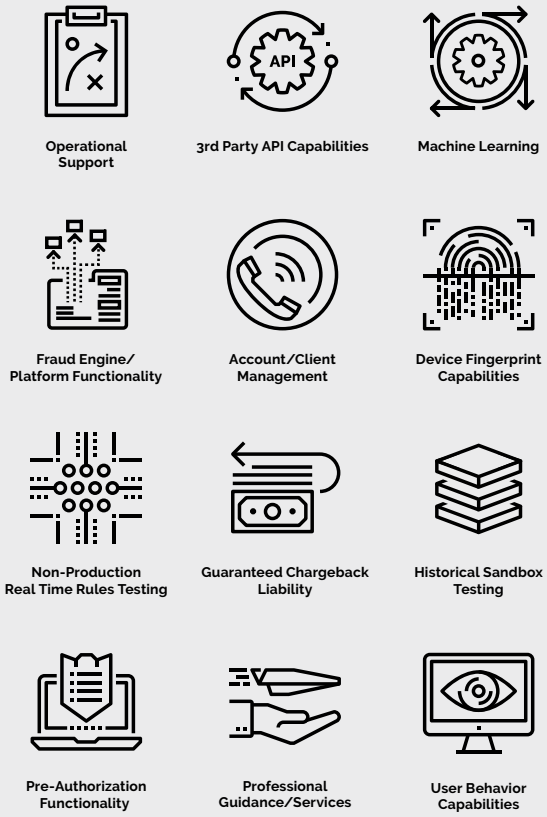
False Declines Cost More Than Fraud

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.

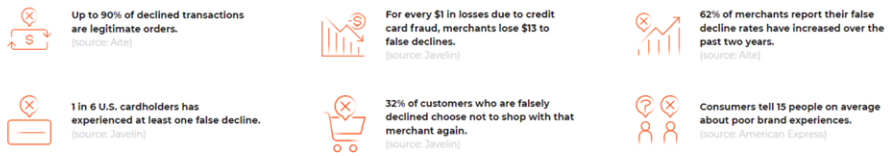
While most ecommerce merchants focus on managing fraud and chargeback costs, the cost of revenue lost to false declines (also known as false positives) is far more expensive.

ClearSale

At a Glance:



ClearSale



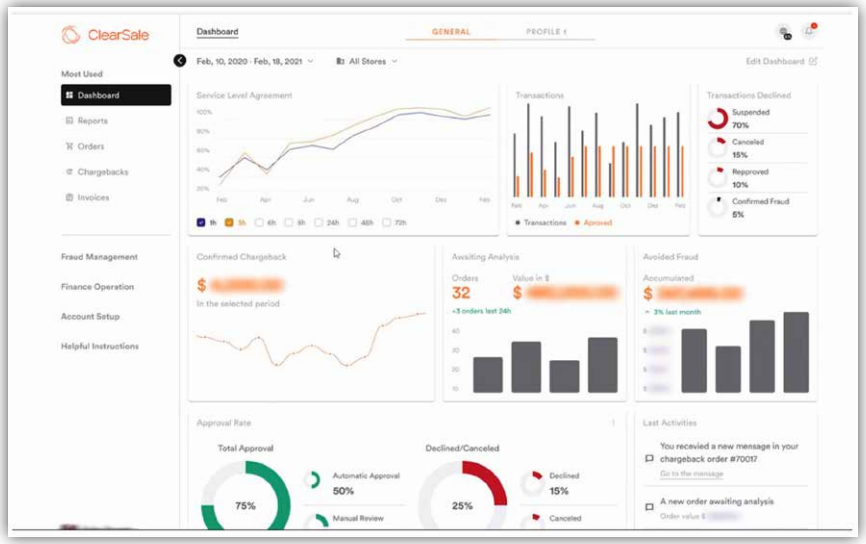
ClearSale's focus on false declines.

Most automated fraud programs are built on fraud scoring and fraud filters designed to catch and auto-decline any order the program thinks might be fraudulent.

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 to their fraud analysis team for further review where the transaction is dissected to validate whether the order is truly fraudulent.

The order must go through two rounds of analysis before it is declined. As a result of this balanced, comprehensive process, businesses should likely experience reductions in decline rates and improved approval rates.



Chargeback coverage options for multiple business models: **ClearSale** offers two forms of chargeback coverage: **Chargeback Protection** and **Chargeback Insurance**. Each approach attempts to provide businesses with comprehensive ecommerce fraud protection, while managing chargebacks slightly differently.

ClearSale Total Protection makes it possible for businesses to recoup a portion of any losses due to fraudulent transactions.

With this solution, **ClearSale** establishes a customized Service Level Agreement (SLA) that identifies specific KPI thresholds. Every quarter, performance is reconciled against those KPIs. If the KPI thresholds are not met, the business receives a discount on its invoice.

In this approach, **ClearSale** provides the full breadth of its ecommerce fraud prevention services to ensure all fraudulent orders are blocked and chargebacks are not generated. However, **ClearSale** does not directly reimburse for any chargebacks that may occur, and the discounts provided are not intended to fully cover any chargeback losses.

Chargeback Protection is best for large businesses with a good understanding of their fraud risk profile and clear documentation of the fraud KPIs behind their ecommerce operations.

ClearSale Total Guaranteed Protection provides 100% guaranteed coverage of any fraud-related chargebacks incurred.

With **ClearSale Chargeback Insurance**, if a transaction is approved that turns out to be fraudulent and results in a chargeback, **ClearSale** pays the entire amount of the chargeback. With fixed per-approved-order pricing, the only cost variabile is sales volume.

Chargeback insurance is best for businesses in high-risk segments or businesses that historically have struggled with high chargeback rates.

How ClearSale Works

While merchants are selling, **ClearSale** is at work in the background, preventing online stores from losing revenue to chargebacks and false declines in real-time.

ClearSale does this with a multi-focus approach: a proprietary A.I. that spots every red flag and questionable action, combined with an expert manual review process that attempts to ensure only truly fraudulent orders are declined.

Here's how ClearSale's full model works:

ClearSale delivers a bespoke fraud solution that fits the precise needs of a company.

You have:	ClearSale can:
Your most profitable products	Prioritize these products across our analytical processes.
Your general customer profiles	Develop procedures to support your customers in the most appropriate ways.
Your VIP customers	Tailor playbooks to offer a higher-level of support for them.
Your target markets	Provide industry-specialized fraud analysts, available 24/7 with multi-language capabilities.

First, a customer places an order.

For clients who are attempting to streamline their business operations and focus more on overall revenue strategy and less on managing fraud risk, **ClearSale** covers all card-not-present transactions, including:

- Web orders
- Email orders
- Virtual terminal orders
- Telephone orders
- Mail orders

Next, the A.I. technology gets to work.

ClearSale's proprietary statistical algorithm scans every order

to detect common fraud patterns. Using fraud rules created specifically for the business and bolstered by a machine learning platform, the algorithm adapts to the unique fraud risk profile.

An extensive amount of data is quickly assessed for each order, including the transactional details of the order, information on the device where the order was placed, known customer behavior, external data sources, historical data, etc.

Once the scan is complete, the algorithm assigns a fraud score for each order.
Orders with a low fraud score are approved immediately. Orders with a fraud score outside of the pre-approved threshold are considered suspicious. These orders are then sent to the in-house manual review team for further analysis which prevents false positives associated with auto-decline decisions.

Finally, an ecommerce fraud analyst manually reviews every suspicious order.
Because suspicious behavior doesn't always mean an order is fraudulent, **ClearSale's** fraud analysts are trained to look for reasons to approve orders — not decline them. If the analyst reviews the evidence and determines the order is legitimate, the order is approved.

If the evidence suggests the order might be fraudulent, it is sent for a second manual review. From there, the reviewer looks at the data elements used to calculate that transaction's fraud score:

- Fingerprint technology to identify computers placing transactions
- Proprietary tracking technology to monitor customer behavior within client websites
- Proxy piercing technology
- Geo-localization
- BIN tracking
- Email intelligence
- CVV verification

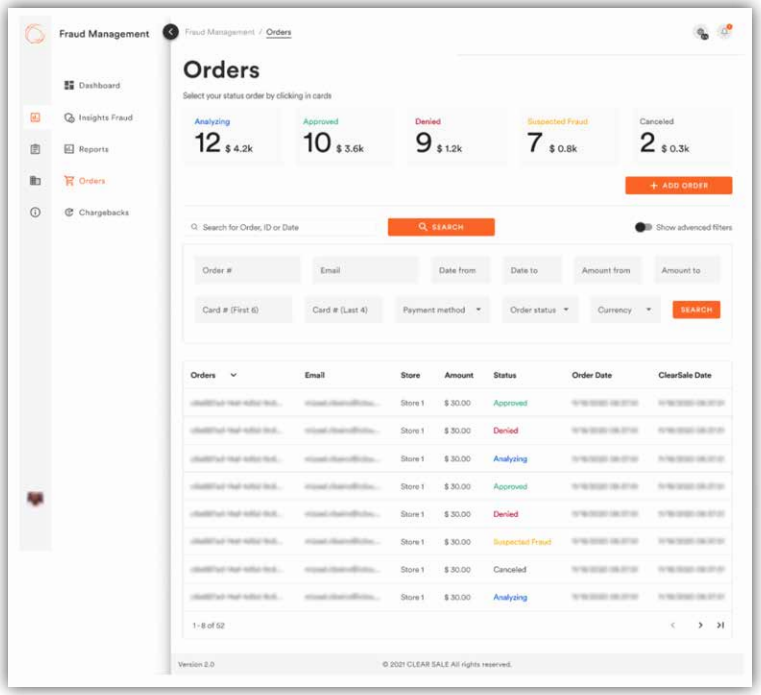
The reviewer then gathers additional insights that may go unidentified by the ML model, but will provide valuable clues to a human being:

- Reverse phone /address lookup
- Social network activity
- Link analysis
- Data visualization

Direct contact with the customer may be necessary using a preapproved call script so customers feel cared for and valued.

If the second analyst determines the order is legitimate, the order is immediately approved. If the second analyst cannot validate the order, only then would it be declined.

ClearSale



About Manual Reviews and Response Times

Based on the notion that manual reviews can impact response times and that some transactions are more urgent than others, **ClearSale's** decision timeframe is customizable. Orders in the system can be flagged for VIP lists and cater decision times to specific industries, countries, and other factors.

Ecommerce Platform Integrations

ClearSale offers ecommerce platform integrations with a wide range of providers which can help streamline the connection. The steps involved are as follows.

1. Retrieve the plugin
2. Enable the **ClearSale** module in the store
3. Keep track of orders on the **ClearSale** dashboard

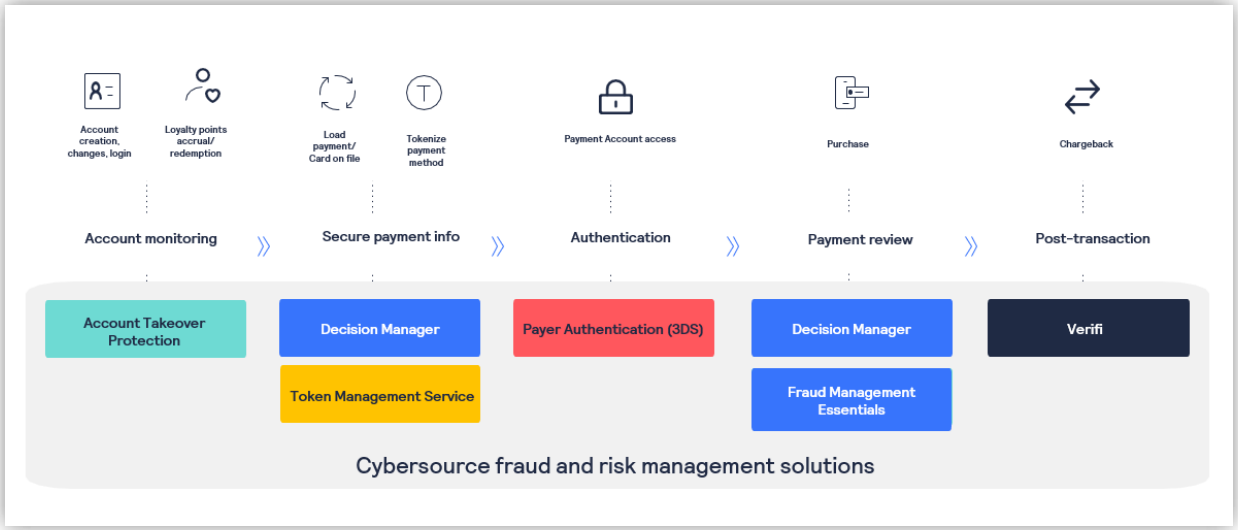
Easy to Implement

Pre-built extensions with most major platforms are available to easily add into your ecommerce system.

shopify · WEBSHOP · Zoey · commerce cloud · nopCommerce · BIGCOMMERCE · volusion · Magento 2 · WOOCOMMERCE · Magento · neto · PrestaShop · shopifyplus · SHIFT4SHOP · ORACLE COMMERCE CLOUD · VTEX

Cybersource

Cybersource is a wholly owned subsidiary of Visa, Inc. Through global reach, modern capabilities, and commerce insights, **Cybersource** creates flexible, creative commerce solutions for everyday life—experiences that delight customers and spur growth globally. **Cybersource** processes billions of secure transactions every year. Each one provides insights to optimize fraud prevention, capture more revenue, and improve customers' authorization rates. Together with Visa's other subsidiary companies, CardinalCommerce and Verifi, **Cybersource** has access to the most modern, secure and optimized payment processes across the payment fraud and risk lifecycle.



Cybersource makes it simple to access all the technologies you need to build global payment solutions your way, all on one platform. They offer payment solutions that are global, innovative, secure, and deliver the payment experiences you and your customers want.

cybersource
A Visa Solution

At a Glance:

- 3rd Party API Capabilities
- Professional Guidance/Services
- Machine Learning
- ATO Detection Capabilities
- Pre-Authorization Functionality
- Fraud Engine/ Platform Functionality
- Account/Client Management
- Historical Sandbox Testing
- Non-Production Real Time Rules Testing
- Operational Support
- Payment Gateway Capabilities
- User Behavior Capabilities

Cybersource

Solutions and Functionality

At the heart of **Cybersource** is a modular, cloud-based platform. Using a single set of APIs, **Cybersource** can integrate with any system in the market and support any vertical: retail, ecommerce, transit, telcos, restaurants, airlines, insurance, and utilities. The modular platform enables clients to:

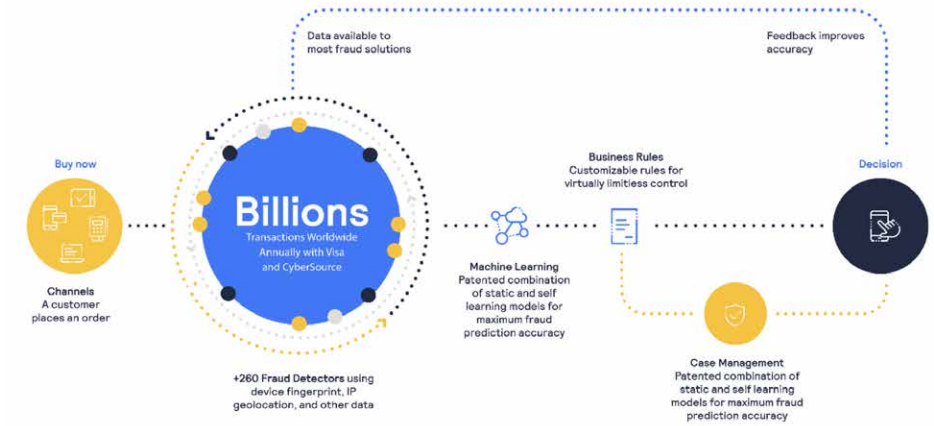
Reach further: Cybersource's global scale enables payments in over 190 countries, and support for over one million users.

Adapt faster: Cybersource's modular services give merchants the flexibility to design a tailored experience for their customers, with payments seamlessly embedded.

Grow stronger: Cybersource was a key player in the ecommerce revolution in 1994 and has been at the forefront ever since. Today, they help over 468,000 businesses to grow and stay protected from fraud.

Manage Risk and optimize revenue

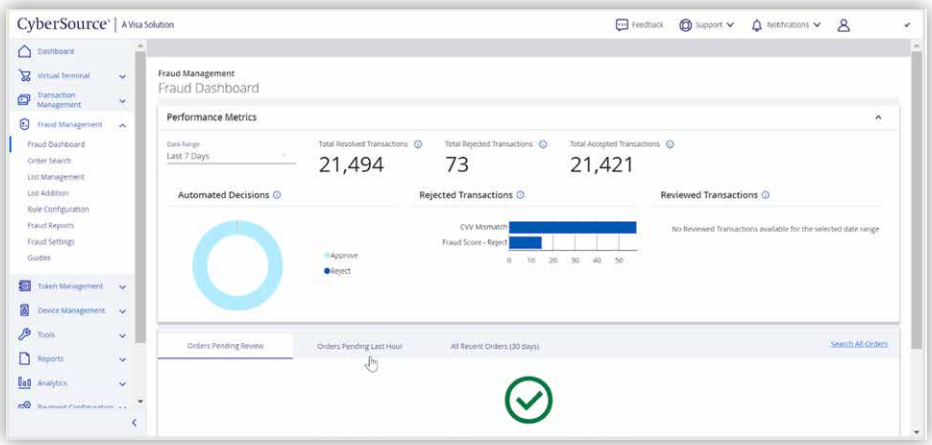
Cybersource processes billions of secure transactions every year. Each one provides insights to optimize fraud prevention, capture more revenue, and improve authorization rates. Its systems are built on proven Visa-grade systems, so data is secure. And **Cybersource's** hands-on experts and award-winning customer services teams support clients at every step.



Decision Manager

Decision Manager is **Cybersource's** award-winning fraud-management solution that keeps fraud low, customer satisfaction high, and revenue flowing. As a fraud detection and risk management tool, Decision Manager allows businesses to accept or reject incoming transactions based on a variety of sophisticated risk models and advanced machine learning detection. It comes fully integrated with payment management or is also available as a standalone service.

Decision Manager automatically analyzes hundreds of data points for each transaction, comparing them against intelligence derived from Visa and **Cybersource's** dataset and with built-in device fingerprinting, IP Address, and biometrics. Their uniquely powerful unified consortium model takes a highly flexible approach to



incorporating and leveraging local-level transaction data at a global scale for greater risk-scoring accuracy — while also anonymizing that data to maintain compliance with strict data privacy regulations and guidelines. Combined with decades of fraud management and data science experience, this unparalleled scale allows **Cybersource** to deliver accurate, automated risk scores that help businesses drive real results.

Decision Manager's extra features:

Decision Manager Replay

Decision Manager Replay is a feature in Decision Manager that allows clients to test new fraud strategies without impacting the customer experience and increase the accuracy, speed, and integration of fraud prevention strategies—helping to plan for peak seasons, reduce manual review, or to communicate differences in various fraud strategies.

Identity Behavior Analysis

Identity Behavior Analysis leverages historical customer identity information across different sellers and industries by using machine learning to automatically identify good, bad, and never-seen-before customers. It allows businesses to optimize each payment and accept more good orders from new and returning customers, based on recognized behaviors, while preventing fraud.

Identity Verification Resources

Decision Manager has also integrated other industry-leading data sources to enhance identity verification. This ensures businesses have access to extra resources to validate transactional information and provide further insights. These sources include Emailage, Perseuss, Credilink, and Targusinfo.

Rule Suggestion Engine

The Rule Suggestion Engine helps clients stay a step ahead of evolving fraud tactics by applying advanced machine learning models to transaction data. The Rule Suggestion Engine quickly identifies emerging patterns and trends and then automatically generates recommended new fraud strategies to improve performance. This means less manual effort analyzing and re-tuning fraud strategies, and more operational efficiency.

Customized Score Builder

Score Builder is a feature of Decision Manager that allows clients

to improve their detection accuracy by customizing the industry-proven **Cybersource** risk score or creating their own score for their business policies. Out of the box, Score Builder increases the accuracy of traditional fraud strategies while minimizing complexity. It does this by empowering businesses to adjust an industry statistical risk assessment to match a score to their specific needs.

Fraud Management Essentials

Fraud Management Essentials helps businesses minimize costly fraud attacks. With ready-to-go fraud filters, businesses can automatically monitor transactions while still providing a seamless customer experience. It's a lightweight and powerful fraud prevention tool to prevent common fraud attacks such as card testing, payment fraud, and common abuse scenarios. The tool leverages Decision Manager with powerful risk models using advanced machine learning and hundreds of validation tests to automate detection and prevent fraudulent transactions.

Fraud Management Essentials provides all the scale, security, and analytics of Visa and **Cybersource**, enabling businesses to grow from SME to enterprise businesses on a single platform. Setup is easy with preconfigured settings that make it simple to get up and running right away and make informed decisions via a user-friendly dashboard.

Account Takeover Protection

Account Takeover Protection identifies and blocks account takeovers, fake account creations, loyalty fraud, and other pre-transaction attacks—all types of fraud that can really damage businesses' reputation. It provides a flexible rules engine to flag and identify suspicious activity based on a customer's behavior, email, device, communications, and other attributes. This enables the service to identify and block account takeovers, fake account creations, loyalty fraud, and other pre-transaction attacks.

Delivery Address Verification

Delivery Address Verification verifies a customer's delivery address during card-not-present transactions. The result set contains an API-specific reply code and a status or error code that is specific to verifying the address. The verification tests produce a valid address along with an estimate of the risk associated with the address ensuring packages arrive at the correct validated addresses, and returned (undeliverable) packages are kept at a minimum.

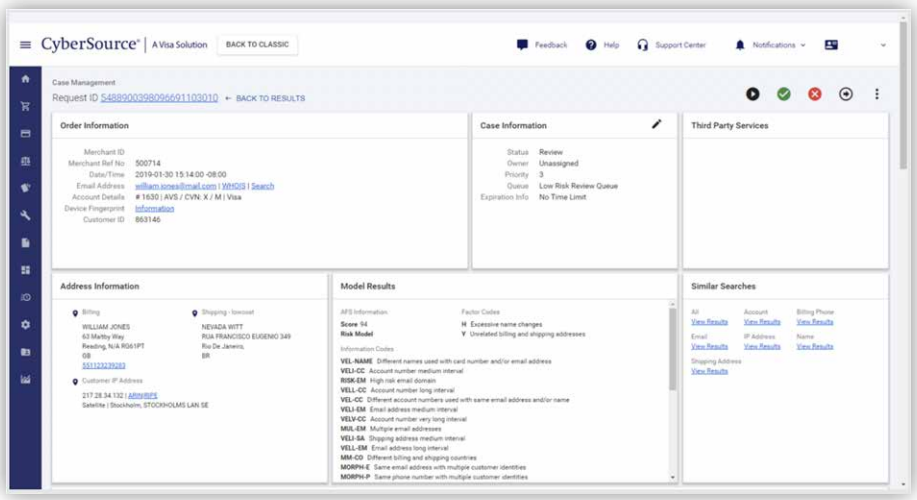
Enhanced Profiling

With Enhanced Profiling, all profiling requests from a visitor's browser will be made to a domain that is secured by a TLS/SSL digital certificate assigned to the client's business. The request is then authenticated with this certificate and provides increased trust between the user's browser/app and fraud prevention.

Watch List Screening

Watch List Screening can help businesses comply with global economic sanctions regulations. Check purchaser information and geographic locations against sanctions and denied-parties regulatory watchlists in real time.

The extra benefit is that order processing carries on seamlessly while watch lists are checked behind the scenes—minimizing delays. And it returns real-time information about purchasers to help businesses make informed decisions about whether to proceed with specific transactions.



Pre-authorization transaction screening through Decision Manager runs Decision Manager prior to authorization, resulting in a "cleaner" set of transactions sent to the issuer for evaluation. Over time, the issuer would analyze, recognize, and establish that a lower rate of declines (active involvement) is warranted for that client since the fraud had been identified beforehand. Running Decision Manager prior to authorization also enables Payer Authentication results within Decision Manager's rule-building capabilities.

Cybersource's advanced machine learning risk models and the power of data expedite fulfillment because they automatically identify good customers, from login to acceptance, providing an end-to-end solution. With Cybersource's industry-leading, innovative approach, clients can rely on our highly accurate risk scores to help guide transaction decisions, get the insights needed to optimize broader risk strategies, and stay focused on core business and optimizing revenue, all while fighting fraud.

Merchant Experience

Cybersource offers different levels of service to support clients' needs.

- An assigned Risk Analyst actively manages risk strategies and **Decision Manager** configurations, in consultation with a merchant, to meet performance metrics.
- An assigned Risk Analyst performs analysis and makes best-practice recommendations; the merchant handles management and configuration of **Decision Manager**.

- Outsourcing of some or all of a merchant's manual review case load, which can include overnight hours, peak season, and high loads during special promotions.

Managed Risk Services

With nearly 70 consultants around the globe—and over 750 years of card-not-present experience between them—Managed Risk Services provides businesses with the expert in-person support that makes such a difference when managing fraud strategies.

Managed Risk Services provides a business with a dedicated risk consultant who helps to maintain their fraud strategies and provide customized insights. They will actively monitor your fraud prevention strategy and apply real-time adjustments based on your business objectives and backed by deep analytics.

Cybersource consultants also operate across our entire client base, allowing them to gain unique insight into fraud patterns, often before a business would. In addition to their consultants, **Cybersource's** Screening Management Team can help reduce overhead by working with business' teams to review transactions flagged for review—helping to reduce false positives and prevent fraud by looking at a customer's purchase patterns.

Managed Risk Services provides various services that are ongoing or one-time engagements tailored to specific business goals. **Cybersource** Managed Risk Services can help stop fraud, reduce operational costs, and increase acceptance in a balanced, business-centric way.

Pricing Model

A variety of pricing options are available to clients, all of which can be influenced by transaction and sales revenue criteria. Supplemental fees may be applicable depending on region, acquirer, and processor requirements. **Cybersource** offers solutions that optimize revenue and minimize fraud based on business needs and goals.

Kount, An Equifax Company

Kount joined **Equifax** in early 2021. Combined, Equifax and **Kount** 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.

Kount's Identity Trust Global Network™ delivers real-time fraud prevention and account protection. It enables customer experiences for more than 9,000 brands and works with over 50 payment processors and card networks. Linked by **Kount's** award-winning AI, the Identity Trust Global Network analyzes signals from 32 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 advanced artificial intelligence, combined with the Identity Trust Global Network, empowers businesses to establish trust or risk in real time throughout every point of 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 in milliseconds.

By combining both forms of machine learning with the Identity Trust Global Network, **Kount** can provide trust or risk decisions in real time. Unsupervised machine learning analyzes potential anomalies and emerging fraud trends faster, more accurately, and on a more scalable basis than human judgment alone. Meanwhile, supervised

Kount®

At a Glance:

- 3rd Party API Capabilities
- Machine Learning
- Operational Support
- Pre-Authorization Functionality
- Account/Client Management
- Device Fingerprint Capabilities
- ATO Detection Capabilities
- Professional Guidance/Services
- Guaranteed Chargeback Liability
- Non-Production Real Time Rules Testing
- Fraud Engine/ Platform Functionality

machine learning analyzes historical fraud data and is trained on **Kount's** Identity Trust Global Network, which includes billions of transactions from over 14 years of data in over 250 countries and territories, as well as more than 50 payment and card networks.

For each transaction, Kount's AI produces an identity trust **Omniscore**, an actionable fraud payments 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.

Kount's Identity Trust Platform gives businesses the control to customize business outcomes by leveraging **Kount's** customer experience and policy engine. **Kount's** flexibility allows customers to maintain control and fine-tune policies based on their industry and business goals. Businesses can lower friction for good customers, increase sales conversion rates, retain customers, and build their brand's reputation.

Products

Kount's Identity Trust Platform can help provide complete customer journey protection, from account creation and login to payment transaction and bot detection. **Kount's** products include:

- **Kount Command™** for payments fraud protection
- **Kount Control™** for account takeover protection
- **Data on Demand**, fueled by Snowflake, for actionable customer insights
- **Dispute and Chargeback Management**, integrated with Verifi, A Visa Solution, and Ethoca Consumer Clarity™, and Ethoca Alerts for managing fraudulent transactions, chargebacks, and disputes

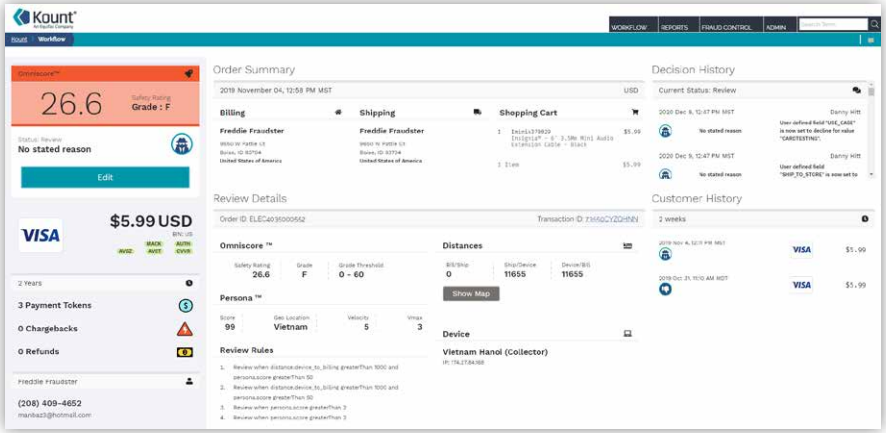
Kount Command protects thousands of leading brands globally, including online merchants, digital businesses, and enterprise-level retailers against digital payments fraud. **Kount Command** also helps businesses reach and maintain desired business outcomes around chargebacks, approval rates, manual reviews, and operational costs.

Kount Command gives customers access to the Identity Trust Global Network, which includes adaptive AI. **Kount's** AI combines supervised and unsupervised machine learning to detect existing and emerging fraud. **Kount's** unsupervised machine learning doesn't require historic data, which can help businesses adapt to changing consumer demands.

Kount Command automates fraud detection, detecting common, sophisticated, and previously unknown fraud attempts in less than 250 milliseconds. **Kount** also allows for flexible control, with a customizable policy engine. Customers can fine-tune fraud prevention decisions, conduct investigations, and monitor performance. They can create policies that meet their unique

business needs and customize risk thresholds to address emerging attack methods and new use cases.

Finally, **Kount Command's** analytics and reporting functionality, Datamart, enables reporting on the rich data points collected from payment transactions, customer interactions, and outcomes. It also allows them to investigate suspicious behavior as well as business performance. That knowledge can improve marketing activities, present up-sell and cross-sell opportunities, present new use cases, and expand sales channels.



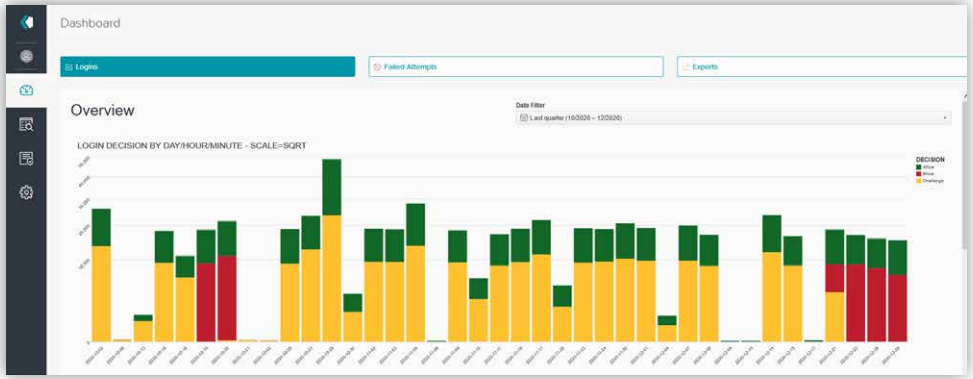
Kount Control account takeover protection aims to provide frictionless account creation experiences, stop malicious logins or account creations, protect against bad and questionable bots, and enable personalized customer experiences. **Kount Control** takes a multilayered approach to account protection: adaptive protection against account takeover attacks, policy customization to fine-tune protection, plus reporting and data presentation to uncover trends. Together, they can reduce false positives, enable customized user experiences, and reveal trends that enrich custom data to inform future policies.

In the protection layer, **Kount Control** evaluates user behavior and device and network anomalies to detect high-risk activity such as bots, credential stuffing, and brute-force attacks. **Kount** then determines, in real time, whether to allow a login, decline it, or challenge it with step-up authentication.

In the policy and customization layer, **Kount Control** customizes user experiences and can help reduce friction by identifying and segmenting users based on common characteristics, such as VIP or trial users. **Kount Control** provides data such as user type, device specifics, IP risk, geolocation, and custom data.

In the reporting and data layer, **Kount Control** provides customer insights that can help fine-tune business policies and customize experiences. Login trend data, including device and IP information, provides the ability to quickly identify and report on failed login attempts, risky IPs, compromised accounts, and inbound anomalies, businesses can stop account takeover attempts. They can also uncover trends that can help enrich their own data and inform future policies.

Kount, An Equifax Company

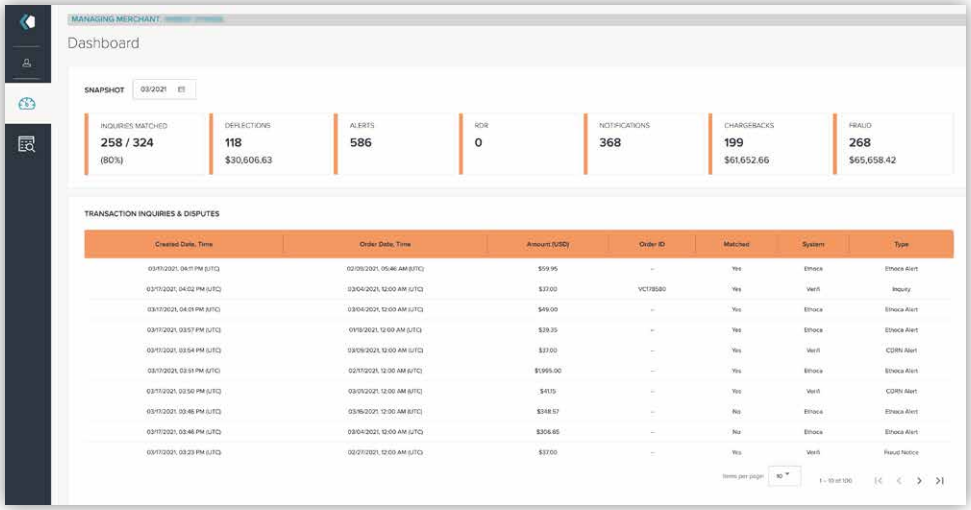


Kount's Data on Demand offers insights to improve customer experiences, reduce friction, increase conversions, and uncover cross-sell and up-sell opportunities. It can enhance a company's customer knowledge with thousands of additional data points from the **Identity Trust Global Network**.

Combining data from multiple sources can help businesses analyze purchase and product usage behaviors to personalize marketing campaigns, products, and services to customers. It can also help businesses approve more good orders and improve fraud prevention strategies. Businesses can analyze the data on its own or combine it with additional company-collected data for deep analytics on one platform. **Data on Demand** was built on Snowflake and is hosted by **Kount** in a private data warehouse.

Dispute and Chargeback Management is a solution that can provide chargeback mitigation and help manage disputes.

Kount has integrated with Ethoca Consumer Clarity™, and Ethoca Alerts, to launch the chargeback prevention solution. Customers can take advantage of chargeback prevention tools to identify, prevent, and resolve chargebacks without the need for development resources or complex integrations. **Dispute and Chargeback Management** delivers all of the benefits of **Kount's** fraud prevention and enhanced capabilities of Verifi and Ethoca's dispute management tools to help stop chargeback losses and reduce dispute timeframes.



Partners

Customers can gain access to the Identity Trust Global Network and **Kount's** solutions by working with **Kount** directly or via **Kount's** partner network. Kount has partnerships with more than

Kount, An Equifax Company

50 payment service providers, gateways, and partners globally, including J.P. Morgan Chase, Barclays, Moneris, Braintree, BlueSnap, and others. **Kount** also partners with ecommerce platforms and payment partners, such as Magento, Shopify, and FreedomPay among others.

Kount's partners access and manage fraud prevention for their merchants through **Kount Central™**, an AI-driven fraud protection suite for online payment processors, payment gateways, hosted payment pages, and ecommerce platforms. **Kount Central** protects payment service providers and their merchant portfolio with AI-driven fraud prevention that uses supervised and unsupervised machine learning. With a single integration, payment service providers can offer a selection of fraud prevention services and use cases.

Features and Functionality

Kount customers can further enhance their fraud prevention strategies with features and functionality such as the following:

- **Event-Based Bot Detection**
- **Email Insights**
- **User-Defined Fields**
- **3DS2 authentication**

Event-Based Bot Detection identifies and segments bots at multiple customer interaction points, including account creation and login, loyalty point or coupon redemption, gift card redemption, and checkout. **Event-Based Bot Detection** examines typical characteristics along with past behaviors and identity trust signals to help understand bot behaviors and determine the trust level of the identity behind the interaction.

When **Kount** identifies malicious bot activity, the data feeds back into the **Identity Trust Global Network** so that other businesses can prevent similar attacks. Using advanced reporting and in-depth insights into customer behaviors, **Kount** can identify bot trends and inform future policies and strategies.

Email Insights can help businesses determine identity trust quickly and accurately. Backed by **Kount's Identity Trust Global Network's** billions of data points, **Email Insights** informs identity trust with data on payments, location, and digital identifiers. In addition to predicting a customer's level of trust, **Email Insights** can help businesses understand a customer's lifetime value and likelihood of making repeat purchases.

Email Insights uses identity trust data to determine an email address's date first seen and date last seen. Knowing the age of an email address can trigger additional friction if needed to authenticate the identity behind the transaction and help prevent

Kount, An Equifax Company

fraud. Further, **Email Insights** helps businesses understand if an email address has been associated with criminal fraud, friendly fraud, or risk.

Their **User-Defined Fields** can help businesses capture details from internal order management systems to analyze orders and improve and automate accept/decline decisions. With more than 500 customizable fields, businesses can capture information that is specific to their products, customers, or goals.

With **3DS2 authentication, Kount** can help reduce customer friction and cart abandonment rates. 3DS2 payment authentication technology protects cardholders against unauthorized credit card or debit use at the point of checkout. By measuring transaction risk through Kount, merchants can customize their risk tolerance levels to approve a low-risk transaction or require additional customer authentication methods.

Professional Services

Kount Professional and Guarantee Services are available for companies who need additional assistance establishing trust and risk management strategies, success measurements, and greater partner collaboration and customization.

Kount's Chargeback Guarantee allows customers to stabilize their fraud expenditures with predictable costs and guaranteed protection against criminal fraud, chargebacks, and losses.

The **Chargeback Guarantee** provides instant approve/decline decisioning with 100% coverage of eligible fraud-related chargebacks.

Kount's Performance Guarantee helps customers focus on achieving specific KPIs by guaranteeing performance on established service levels.

Kount's Policy Management and Optimization (PMO) is designed for customers who anticipate or experience sophisticated fraud attacks, have complex business problems that aren't third-party fraud, or seek additional fraud prevention guidance. **PMO** provides performance analysis and ongoing management and optimization of business and operational policies.

Kount's Managed Services help customers who need to build internal fraud expertise or reallocate resources to activities that aren't day-to-day fraud prevention operations. **Kount's Managed Services** include implementation of **Kount's** solution, from the creation of business policies to manual reviews. **Kount's Managed Services** allow businesses to gain value from **Kount's** experienced fraud experts and hand over fraud-prevention decisioning to them.

Kount's Consulting Services provides access to a broad team of fraud professionals with expertise across multiple industries

and specialties. Businesses gain training for fraud analysts on manual review best practices, progress reporting, and expert guidance regarding control measures to implement throughout the customer journey.

Customer Success Managers deliver personal and immediate support to **Kount** customers. They specialize in product integrations and business setup and can support a business' day-to-day operations, which includes business policy creation and client-specific questions. **Customer Success Managers** also have access to **Kount's** Data Science and Data Analytics teams, as well as third-party partners for expanded services. **Customer Success Managers** work with business' fraud teams on education, strategy development, business policies, and training.

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.

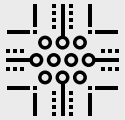
Data management is one of the most critical areas of focus. One of the reasons anti-fraud and AML have habitually operated in isolation is that often the data sources are in different systems, owned by different parts of the organization. Effective financial crime prevention requires synergies across people, processes, and technology.

NOTO

YOUR DATA. YOUR WAY. NO LIMITS.

At a Glance:

Account/Client Management



Non-Production Real Time Rules Testing

Fraud Engine/ Platform Functionality

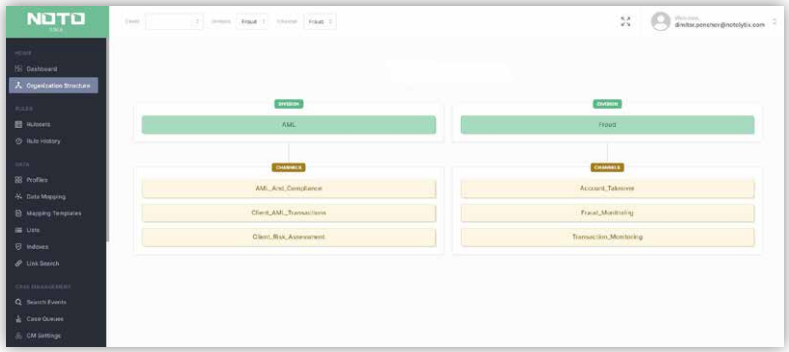
Professional Guidance/Services

NOTO

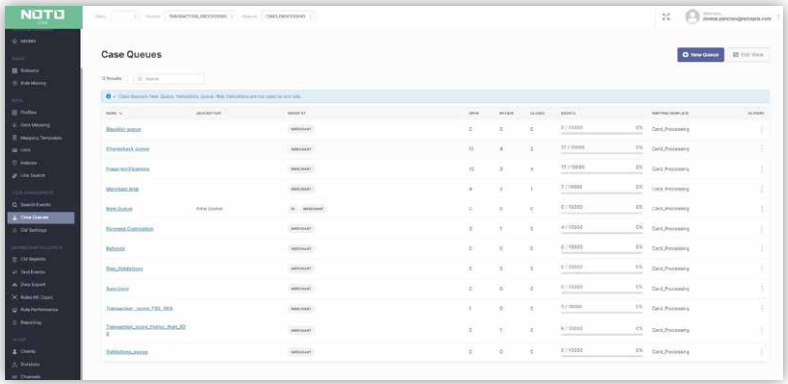
Other areas of attention should include centralized case management, risk assessment, and customer experience, all of which are equally important to building a successful business. Deploying a centralized financial crime prevention solution is of paramount importance to scaling sales and operations.

NOTO helps companies to consolidate information from all data sources and provides real-time monitoring and alerts to help organizations to quickly reference high risk user behavior and transaction patterns.

NOTO is truly data agnostic, fully user-customizable and user-friendly. It provides real-time detection of fraud and money laundering across all business verticals and user interaction channels.



The solution provides relevant applications for a range of verticals including banking, gaming, crypto exchange, fintech, and payment processing. **NOTO** excels in verticals where new regulations are constantly raising the degree to which organizations must manage AML and fraud controls. Additionally, PSD2 has triggered a rapid evolution in the banking industry, bringing instant transfers and open bank APIs that further complicated the banks risk profile.



AML Solutions

- **Initial and ongoing customer risk assessment:** Develop, deploy and tune any in house proprietary risk assessment matrix for initial and ongoing risk assessment for all types of customers.
- **PeP and sanctions screening:** Conduct highly accurate and custom screening of the customer base with fully integrated industry leading third-party vendors.
- **Omni-channel Transactional AML:** Expand compliance oversight into any user interaction channel. Identify previously unidentified links between accounts by tapping into online banking interactions and non-financial user activity.

NOTO

Fraud solutions

- Omnichannel payment fraud prevention
- Account fraud (account compromise and fake account registration)
- Internal fraud
- Loyalty abuse

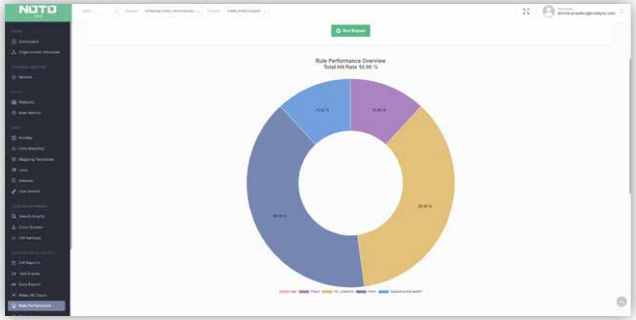
Services

The team of experts in compliance and fraud prevention is able to assist organizations with a wide range of projects. In particular, the team will be helpful for those looking to scale a business with compliance, fraud and payments operations in mind and those without in-house resources on hand. NOTO offers the solution as well as a team of analysts to help manage all aspects of compliance monitoring on a daily basis.

Reporting options

Case management reporting:

- Number and frequency of alerts
- Case resolution by typology
- Resolution time
- Review time
- Analyst and team performance



Fraud reports:

- True/false positives
- Eventual manual resolutions
- Specific Rule Response
- Extensive export functionality
- Opportunity to feed all reports and meta data into client BI tools

Proof-of-Concept process:

This typically includes access to a test environment as well as the opportunity to share existing use cases (for fraud or compliance). An anonymized data sample is typically provided, from which outcome responses are provided which can then be compared to actual outcomes.

Pricing format:

NOTO provides two ways of deployment–SaaS and on-premise. Depending on the deployment strategy, different pricing applies. The pricing is largely based on usage and use-cases within

the platform. **NOTO** can be rapidly deployed (in cases of SaaS deployment), and organizations can benefit from the platform's capabilities after a short implementation period.

Integration:

Depending on client export accuracy, integration generally takes 4-6 weeks for SaaS, with an 8 to 12 weeks integration period for the on-premises option. This is all followed by 2-3 weeks of output review.

12 Month Roadmap

- Ability to train models in environment–no secrets around what's good and bad
- Ongoing improvements in case management
- Adding third parties
- Reporting component described previously–modular reporting
- Visual link search–also received in an actionable list

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.

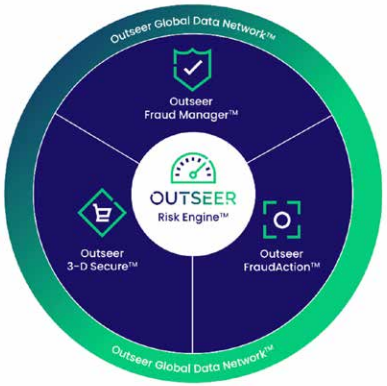
Outseer supports Key Performance Indicators (KPIs), including:

- Increased transaction approval rates
- Improved customer loyalty by providing frictionless digital experience
- Reduced fraud losses
- Lower False Positive ratios

Products, Solutions and Technologies:

Outseer provides a range of products and solutions to enable issuers, payment processors, and merchants worldwide:

- **Outseer FraudAction™** is a managed service that delivers rapid detection and takedown services related to phishing, rogue apps, and fraudulent social media activities. It also offers data insights into threat activities on the dark web to protect customers and an organization's brand.
- **Outseer Fraud Manager™** protects customers across all digital channels with risk-based account monitoring



OUTSEER
An RSA Company

At a Glance:

- Machine Learning
- Device Fingerprint Capabilities
- Account/Client Management
- Non-Production Real Time Rules Testing
- Professional Guidance/Services
- Pre-Authorization Functionality

solutions, detecting 95% of fraudulent transactions with only 5% intervention.

- **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™** (announced February 2022): 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™:

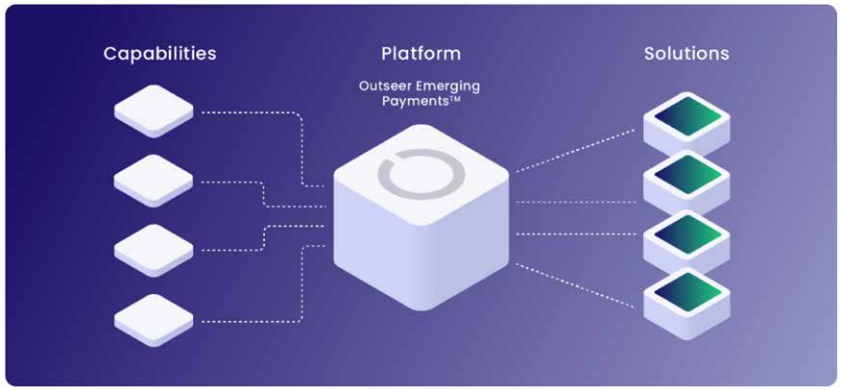


Figure 2: **Outseer** Risk Engine

The **Outseer Risk Engine™** underlies **Outseer** products and solutions. It assesses more than 100 different fraud indicators to evaluate the risk of a transaction in real time and produces a risk score. The score is based on a number of different contextual data elements, including device and behavioral profiling data elements from the 3-D Secure protocol where applicable, and intelligence from the **Outseer Global Data Network™**.

The **Outseer Risk Engine** uses a machine learning, statistical approach to calculate the risk score. This approach examines the conditional probability of each event to evaluate if it's most likely genuine or fraudulent given known facts or predictors. All available factors are considered and weighed according to relevance, so that the most predictive factors contribute more heavily to the score. The predictive weighting calculations are updated daily based on the feedback from case management, chargeback data, and authentication results.

The **Outseer Global Data Network** is a shared global, cross-industry anti-fraud intelligence network used to inform risk decisions. Network members use the **Outseer** case management application to mark activities as "Confirmed Fraud" or "Confirmed Genuine"; once marked, the associated data elements are shared across the network. When an activity is attempted and includes one of the elements from the Global Data Network, the risk is automatically adjusted.

Reporting & Analytics:

Outseer 3-D Secure and **Outseer Fraud Manager** provide reporting via an online dashboard, available in a range of formats. Visualized, pre-defined reports are available, including but not limited to: transactions, rules analyses, step-up authentication analyses, case markings and many more.

In addition, **Outseer 3-D Secure** and **Outseer Fraud Manager** Raw Data Reports are available daily for download, allowing customers to consume the raw data into their data lakes/data warehouse for further correlation with other data sources.

Outseer FraudAction includes access to an online dashboard for visualizing the attack trends and service elements like shutdowns, status, and data feeds. The data is available for download or via APIs.

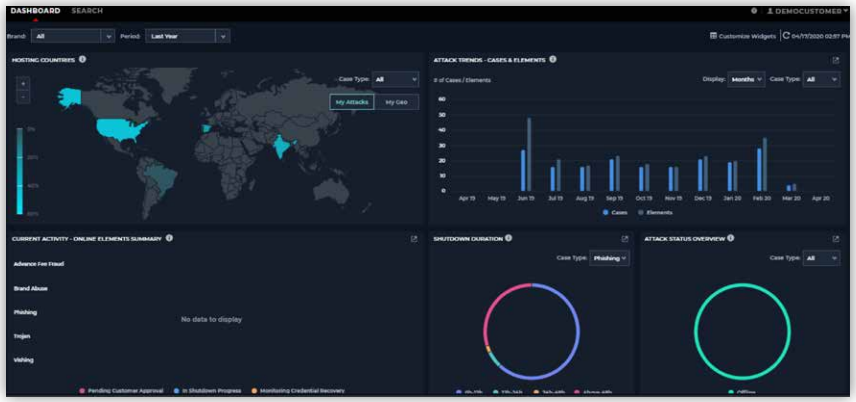


Figure 3: Outseer FraudAction Dashboard

Proof-of-Concept (PoC) Processes:

The **Outseer** approach to PoC varies for the different product. For example, an **Outseer FraudAction** PoC will include providing samples from the dark web and malicious URLs targeting the prospect organization. For other products, the PoC process is customized and may include aggregated, anonymized proxy performance and results based on Outseer's previous experiences.

The **Outseer Risk Engine, underlying Outseer products**, efficiently learns to provide a fully tuned risk calculation based upon the customer's specific use cases and implementation. During the initial learning period, the **Outseer Risk Engine** takes into account a number of factors and provides customers the option to tailor inputs, business rules and other implementation considerations. This allows customers to evaluate in "test mode" to understand the impact of different rules and conditions prior to being deployed in production.

Integration:

Integrating with **Outseer Fraud Manager** includes implementing APIs that trigger the risk assessment process and the step-up authentication flows.

Outseer Global Services supports customers throughout the implementation phase. The complexity of the implementation depends on the number of step-up authentication options (and

types) that a customer implements and the number or channels and event types (such as different payment types) that the customers chose to protect with the product.

Outseer FraudAction is a managed service and does not require implementation on the customer end; only requires setup by Outseer's which typically completed in less than two weeks.

The **Outseer Beyond** partner program, a program for complementary providers of payments authentication and fraud prevention technologies, further extends Outseer fraud, risk and identity capabilities.

Client support options:
Outseer offers full-time application support. Through Professional Services, **Outseer** also has flexible Technical Account Manager options, offering on-site assistance in 25%, 50%, and 100% commitments per annum.

Through Professional Services, **Outseer** also offers Fraud Data Science services including access to specialists who assist customers in analyzing deep product and performance trends such as analyses of different fraud vectors or product performance indicators in order to recommend product and fraud management strategies and optimization opportunities.

Ravelin

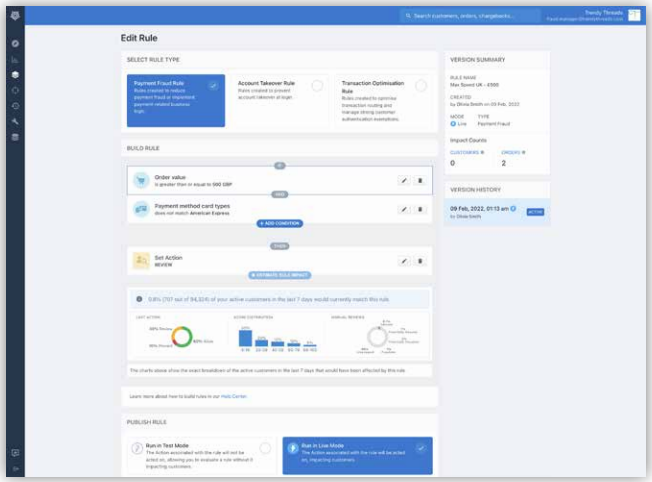
Founded in 2014, **Ravelin** works with ecommerce retailers, online marketplaces, fintechs, and financial institutions by request. They operate in 185 countries, producing over six billion fraud scores annually (through both direct and indirect integrations). They help predict risk with accuracy and 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.

Ravelin supports focus and improvement on the following performance indicators:

- Chargeback rate
- Acceptance rate
- False positives
- Successful logins

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



At a Glance:

- 3rd Party API Capabilities
- Operational Support
- Machine Learning
- ATO Detection Capabilities
- Account/Client Management
- Device Fingerprint Capabilities
- User Behavior Capabilities
- Professional Guidance/Services
- Pre-Authorization Functionality
- Fraud Engine/ Platform Functionality
- Non-Production Real Time Rules Testing

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.

The areas with full solutions include:

- Account takeover prevention
- Voucher and policy abuse
- Loyalty abuse
- Marketplace supplier fraud
- Bot detection and mitigation

In addition to fraud, **Ravelin** also offers payment solutions which can be used to navigate PSD2 regulation. These include:

- 3DS server for PSP agnostic authentication for large merchants, up to version 2.2 exemptions management
- TRA capabilities

Reporting options:

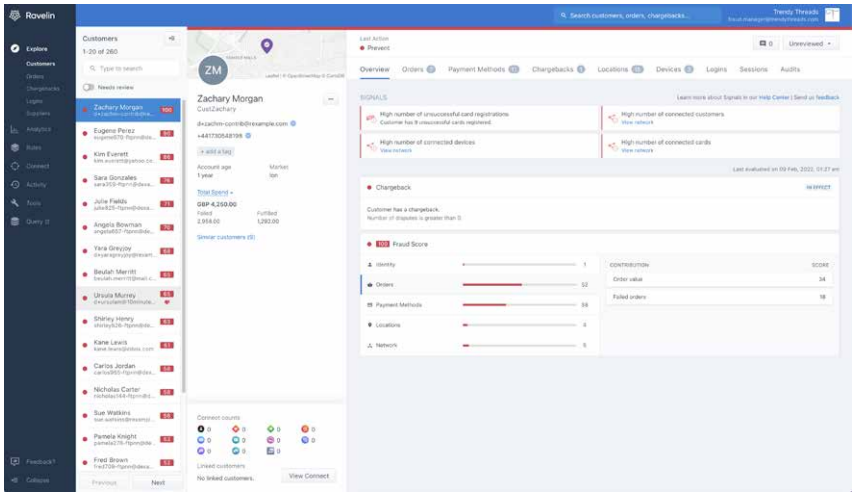
In-app, there are a large number of standard reports (listed below). A report builder also exists, which allows an admin to build their own reports based on 40+ parameters. Outside of the app for enterprise clients, custom reports are available from the investigations team. They're built from core data that can investigate or predict specific concerns or emerging trends.

Fraud Reporting Overview

- 90 Day Chargeback Rate
- Daily Chargeback Rate
- Chargeback Value ($USD)

Ravelin

- Chargeback Count
- Chargeback Rate by Card Schemes



Customer Reporting Overview

- **Last Action - Customers:** The percentage of active customers per day, by Last action
- **Prevent Sources - Customers:** The percentage of active customers with a "Prevent" Last Action per day, by action source
- **Last Action - Orders:** The percentage of order per day, by Last action (Allow Prevent Review)
- **Prevent Sources - Orders:** The percentage of orders with a "Prevent" Last Action per day, by action source
- **Login Status:** The percentage of login attempts per day, by login status (Successful/Failed)
- **Login Count:** The count of login attempts per day, by login status (Successful/Failed)
- **Authentication Mechanism:** The percentage of login attempts per day by authentication mechanism
- **Breached Credentials at Login:** The percentage of login attempts per day using credentials that appear in Ravelin's breached credential database
- **Last Actions - Successful Logins:** The percentage of successful logins per day by Last Action (ATO, Permit/Block)
- **Transaction Optimisation Overview:** The rate of successful authentication attempts per day
- **Authorisation Rate - By card scheme:** The rate of successful authorisation attempts per day
- **Frictionless authentication count:** The count of frictionless authentications by 3DS version
- **Soft decline count:** The count of successful authorisations after a soft decline by issuer

Proof-of-Concept process: Ravelin is available to run side-by-side with an incumbent solution in a proof of concept with live data to compare accuracy and acceptance levels. Alternatively, historical data can be sent offline and assessed though it is usually at a degraded accuracy versus live data. Ravelin is keen to make any merchant comfortable with their decision to switch.

Ravelin

Pricing format: Includes an annualized fee billed monthly that is usually based on the monthly transactions volume of the merchant. Additional services (such as ATO, refund abuse, transaction optimisation, or voucher abuse) can be priced into the monthly fee or can be added later at an additional fee.

Integration: Integration takes place directly with the **Ravelin** integration team. It's usually a two- to four-week process depending on its complexity. There is then an option of a darkmode go-live to validate the recommendations, or a client can go live immediately upon completion of integration.

Current time from signature to go-live is targeted at four weeks.

Integration Guides can be found here.

Support available:
All enterprise clients receive full support from **Ravelin**, including a mix of:

- Direct access via Slack to support team
- Regular meetings with both support and investigations teams
- Dedicated account manager
- Quarterly meeting and reports
- Access to a data warehouse for self-run reports (additional fee)

12 Month Roadmap
Ravelin operates a rolling release schedule with constant improvements to the core product.

- Other highlights expected this year include:
- Extended bot mitigation capabilities
- Extended account security capabilities with a single risk score for multiple fraud types
- Extended ML modeling approaches for new and emerging fraud risks
- Enhanced rules engine for additional flexibility
- Additional user-driven reporting in-dashboard
- Fuller case management capabilities and additional investigation capabilities for fraud agents
- Additional use cases for Ravelin Connect graph network
- Full certification from 3DS 1.x and 2.x server capabilities
- Delegated Authentication for PSD2

Sift

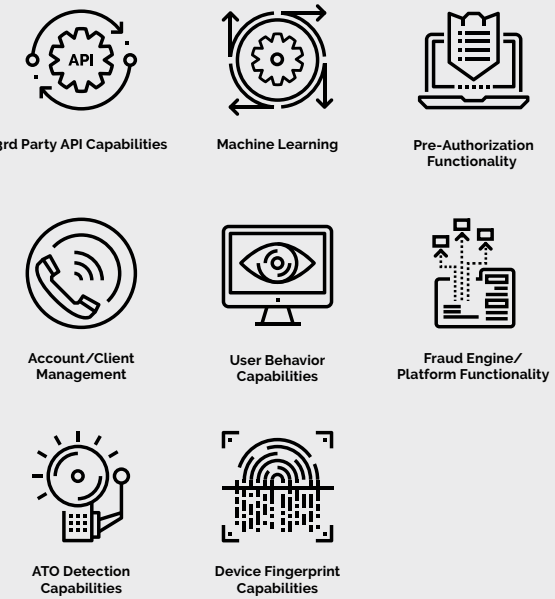
Sift is focused on Digital Trust & Safety, empowering businesses of all sizes to defend against fraud and abuse while fueling rapid growth. Some of the largest merchants in the world—including Twitter, DoorDash, and Wayfair—trust **Sift** to help deliver positive customer experiences, lower chargeback rates, and proactively prevent online fraud. With real-time machine learning, up-to-the-second signals from a global network of merchants, and a worldwide community of fraud fighters, **Sift** is committed to building long-term partnerships and helping businesses gain, and maintain, competitive advantage in their respective markets.

Solutions & Functionality

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 along the way so merchants can automate and scale fraud operations, and make instant and accurate decisions. 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 highly accurate risk assessment of the trustworthiness of an interaction.

At a Glance:



Sift

Sift combines global models with custom learning and extensive feature engineering to deliver accuracy and enable dynamic, real-time decisioning. The global models anonymously share insights about new, emerging fraud patterns across the network, significantly boosting prediction accuracy. These global models are blended with custom models designed to 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 pieces to generate tens of thousands of signals across identity, device, behavioral, and transaction vectors. This all happens within milliseconds, enabling instant action—from automatically blocking or accepting transactions to dynamically tailoring the level of friction applied in the user journey.

Sift's products are scalable and flexible, and can serve as either the primary fraud tool for a business, 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. The Console gives trust and safety teams of all sizes everything they need to investigate fraud patterns, automate decisions, conduct swift and accurate manual review, and analyze business performance. It also supports capabilities for greater protection and growth with multi-factor authentication and decision optimization false-positive experimentation.

Sift offers a comprehensive set of fraud and abuse prevention solutions in its Digital Trust & Safety Suite. Each solution is powered by its own set of use case-specific machine learning models and risk assessments. All products are enabled and accessible through a single, integrated, web-based Console. Products include:

Payment Protection

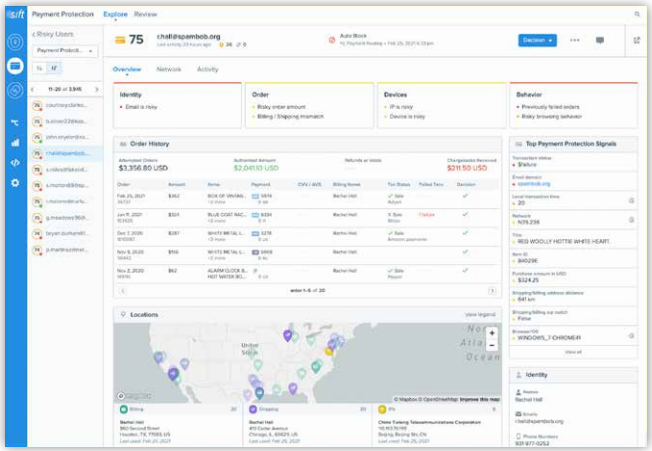
- Proactively stop all types of payment fraud, including fraudulent chargebacks, to protect revenue
- Block fake accounts and risky signups
- Streamline operations and reduce time spent on manual review with case management, automation, and reporting
- Drive growth by accepting more orders and enabling seamless transactions

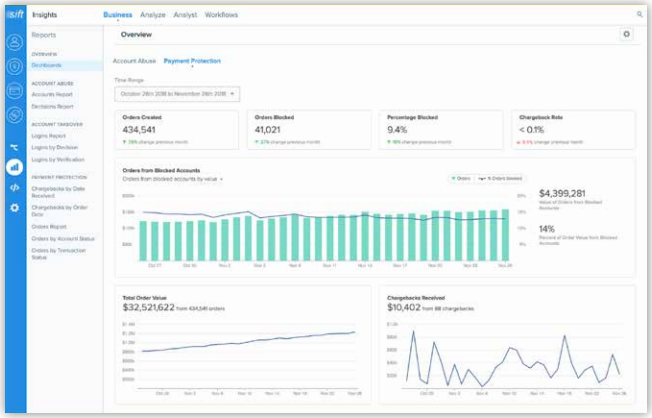
Account Defense

- Stop account takeover attempts to secure trusted user accounts and stored value
- Apply multi-factor authentication (MFA) and security notifications to protect users' accounts
- Dynamically reduce friction for trustworthy sessions

Content Integrity

- Proactively block spam, scams, and other malicious content
- Block inauthentic or duplicate accounts and risky signups
- Create positive user experiences to strengthen trust in your brand and drive growth
- Build automation, review risky cases, and remove malicious content at scale





Sift's single, web-based Console capabilities include:

- **Case management and network graph: Sift** provides machine learning insights in a visual interface, so analysts can understand the reasoning behind each **Sift** assessment and expedite manual review decisions. This includes risky signals, locations of IPs, order and content history, and a network graph that shows signals shared across multiple users.
- **Manual review queues:** Customers can queue users, orders, or content for manual review based on customizable criteria that leverages the **Sift Score** and other fraud signals. Queues automatically assign open cases to individual analysts, while avoiding overlapping reviews. These queues also support escalation for additional rounds of review by senior analysts or managers.
- **Automated Workflows:** Trust and safety teams can automate decisions and business processes by defining automated Workflows based on criteria using "if/then" analysis. Workflows are completely customizable and can be, for example, configured to automatically reject risky users, reduce friction for trusted users, assign transactions to analysts for manual review, and initiate additional verification processes such as 3D Secure and SMS verification.
- **Customizable roles and permissions: Sift** supports multiple user types with a wide range of permissions depending on

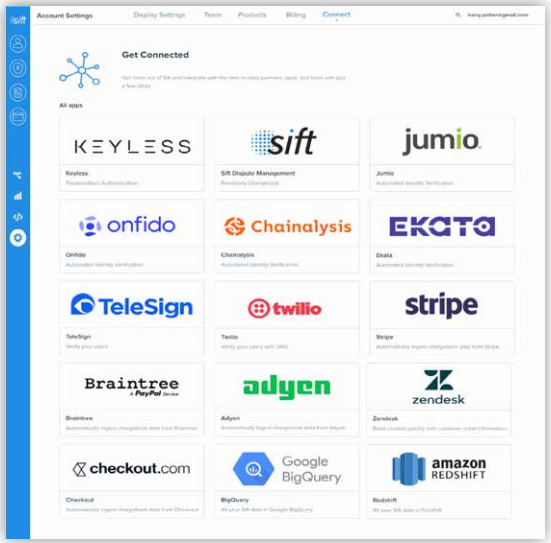
the requirements of their role. For example, admins may have access to manage Workflows, analysts may have access to order details and the ability to make decisions, and a developer may only have access to integration health information. Customers can configure custom permissions to suit their team needs.

- **Multilevel account support:** Customers can set up sub-accounts within a global account to support multiple business units and geographic regions. Sub-accounts are easy to jump between, and a global view provides aggregated insights across all sub-accounts.
- **Real-time analytics:** Admins can track business health with comprehensive insights that report on different criteria, such as order block and acceptance rates, chargeback rates, and risky signups.
- **Built-in Verification & Authentication:** Customers can easily set up email or SMS notifications within the Workflows environment to authenticate any risky signals or transactions that need an additional check.

Sift Connect

Sift Connect is the central hub for Digital Trust & Safety app integrations. Using apps and open APIs, organizations can integrate faster, improve accuracy and efficiency, and share actions across departments.

- **Low- and no-code integrations:** Trust and safety teams can quickly get up and running with **Sift** using connectors to popular digital commerce platforms, such as Shopify, Magento, and Salesforce Commerce Cloud.
- **Consolidated data and tools:** Apps make it easy to ingest data from other solutions such as PSPs and third-party data providers. Once an app is installed, the data is available within the Console—reducing the number of tools analysts need to switch between to do their jobs.
- **Higher levels of transparency:** Integrating valuable fraud data from **Sift** with other business data in data clouds and business intelligence tools enables more flexible reporting, and breaks down data silos across teams—from customer support to finance, business operations, and product.



Sift

Services Offered

New customers have a dedicated Account Executive and Solutions Engineer to ensure successful integration and onboarding. Each integration is handled on a case-by-case basis and customized to use case and business model needs. Customers are also assigned a Technical Account Manager for ongoing support, including continued training, additional integration assistance, and regular maintenance.

A team of Trust and Safety Architects, all of whom are industry experts, are available for consultation to help teams of all sizes craft a holistic, scalable Digital Trust & Safety strategy. Support Engineers are also available to answer any questions about product usage and technical details. Integration, account management, regular support, and trust and safety assessments are all included. Premium support plans can be purchased based on volume and need.

In development in the next 6-12 months:

- Optimized integration and tooling for the unique needs of PSPs who service several merchants across various industries.
- Expanded range of authentication options for Sift Account Defense customers.
- Expanded Workflows/Rules capabilities, including new analytics.
- Improved network visualization and reporting capabilities.
- Integration with popular KYC solution providers.

Signifyd

Signifyd's Commerce Protection Platform recognizes the true identity and intent behind every payment, protecting shopper journeys globally and restoring mutual trust between merchants and their customers. **Signifyd** works with a large number of enterprise customers—including two of the world's top three online retailers. They are headquartered in San Jose, CA., with locations in Denver, New York, Mexico, Belfast, and London as well.

Signifyd helps merchants:

- **Protect revenue:** At every stage of the customer journey, there are conversion drop-offs that reduce the revenue potential of any given shopper. To name a few, this includes pre-auth declines by issuing banks, declines within the fraud management process, the lost revenue due to consumer abuse manifesting as returns, and chargebacks. **Signifyd** helps in analyzing and optimizing these conversion points. They provide benchmarks of comparable ecommerce businesses to diagnose priorities when it comes to enhancements, and they help in implementing the enhancements needed to improve the end-to-end funnel.
- **Trust customers:** The new generation of consumers expects more from their shopping experience than ever before. Friction is not tolerated, and as merchants begin to compete on their customer experience, it becomes crucial to offer a fast and secure checkout, real-time updates on order progress, and avoidance of step-up authentications. **Signifyd** unlocks these differentiating shopping experiences for merchants by providing a foundation of trust—99% of orders **Signifyd** processes are placed by shoppers they've seen before.
- **Grow fearlessly:** When merchants are liable for fraud, they are forced to make decisions based on fear – and fear stifles growth. By shifting liability away from

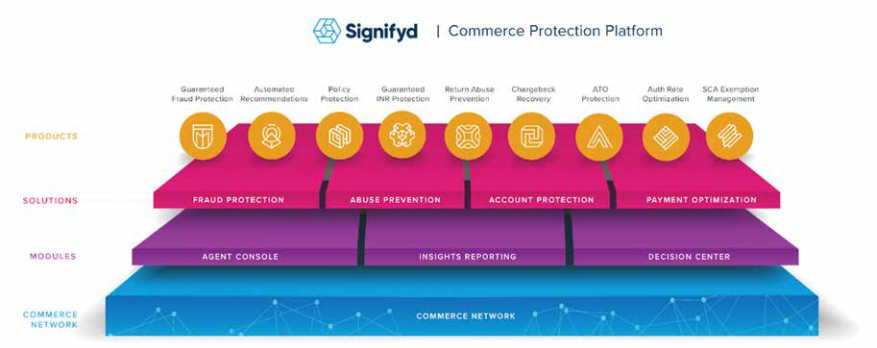
Signifyd

At a Glance:

ecommerce merchants, **Signifyd** eliminates the roadblock of fear and clears the pathway for fearless growth. Empowered with the knowledge that they will never pay another fraud chargeback on an approved order again, merchants can confidently launch new products, expand internationally, adapt to local and regional regulations, offer omnichannel shopping experiences, and establish flexible business policies and customer rewards – all while automating at scale.

Platform, Solutions, & Functionality

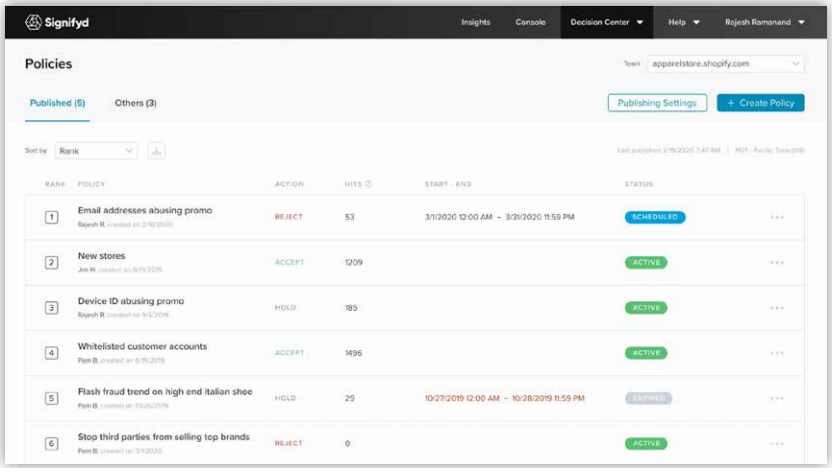
Signifyd's Commerce Protection Platform is designed to provide the tools necessary for merchants to build mutual trust with customers by eliminating fraud and protecting the shopper journey.



Signifyd's Commerce Network: As the foundation of the Commerce Protection Platform, the Commerce Network unites identity and intent intelligence data from thousands of global ecommerce retailers with PSP data, issuer insights, and merchants' own consumer data to proactively block emerging fraud and abuse trends. With 99% of online purchases today made by consumers previously seen across the Commerce Network, legitimate customers are instantly recognized and accelerated down their path to purchase.

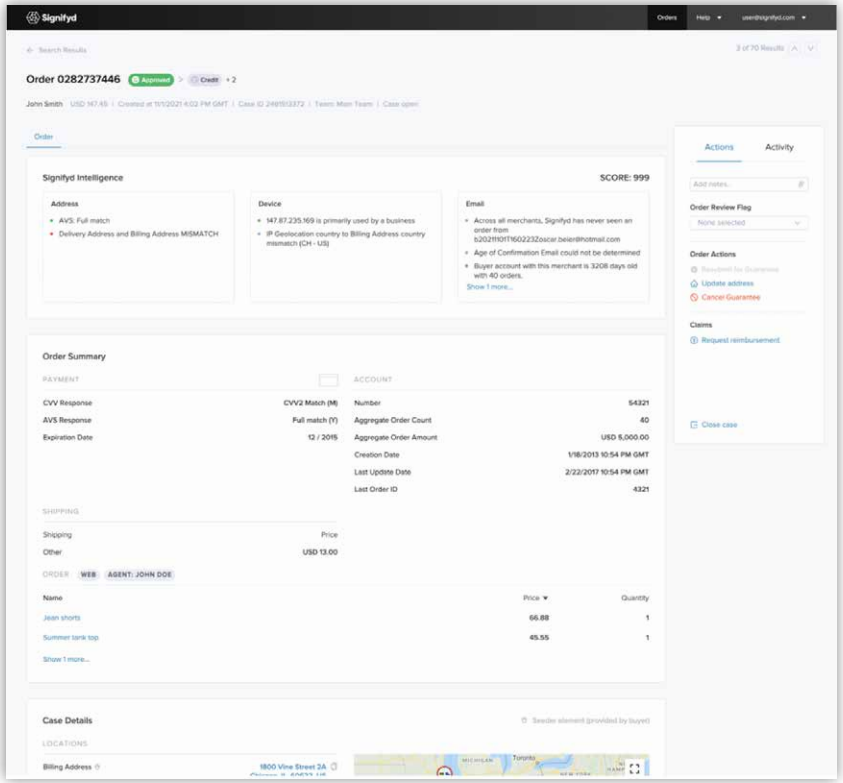
Signifyd's artificial intelligence and machine-learning engine is driven by a combination of both supervised and real-time machine-learning models, using XGBoost, FastText, and other proprietary algorithms. **Signifyd** has built a library of thousands of features over the last decade including those that look at velocity, linking, aggregation, and other areas relevant to risk management. The company runs multiple models in parallel and leverages their results depending on specific customer needs for automated decisions or scores.

The platform features three core modules, which provide a window into **Signifyd's** network and engine: **Decision Center** to create and enforce custom business policies, **Agent Console** to view transaction-level information and variables used to inform decision making, and **Insights Reporting** to provide the business intelligence and benchmarking necessary to optimize performance over time.



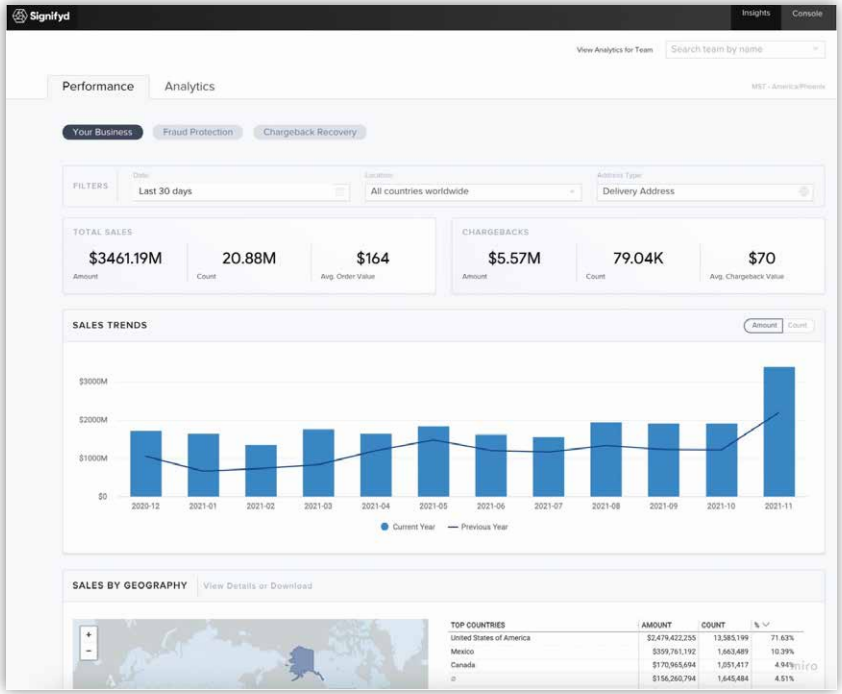
Similar to the need for transparency into decisions, merchants migrating to machine learning from rules-based platforms want to maintain control over their unique business policies and the customer experience they drive. And no one knows a merchant's brand better than the merchant themselves. **Decision Center** puts the power of the Commerce Network into the hands of the merchant, allowing their risk or fraud management team to draw on network insights as well as business-specific data when creating and enforcing policies specific to their business. Merchants can create, test, deploy, and manage all of these policies directly from **Decision Center**.

Agent Console is an interface that gives agents visibility into transaction-level data. Agents can drill into the data variables used to inform order decisions made by **Signifyd's** machine-learning



model, as well as indicators into which variables weighed most heavily into decisions—both positive and negative. **Agent Console** also gives agents the ability to make modifications to an order (i.e. update delivery address) as well as to submit claims for any orders that have been covered by our liability. As merchants make the shift from legacy rules-based solutions to machine-learning platforms, the transparency provided by **Agent Console** builds merchant trust in **Signifyd's** decisioning model and allows merchants to discover patterns that may indicate emerging fraud trends.

Signifyd



Insights Reporting allows business users as well as data analysts to drill into transactional data and track business performance across segments such as geographies, product lines, or payment methods. **Insights Reporting** also comes with Chargeback Insights for customers leveraging **Signifyd's** automated Chargeback Recovery service which monitors chargeback rates, trending chargeback reasons, and win rate of chargeback representment over time. The module includes a fully functional user interface to visualize these insights and interact with the data dynamically in real time.

In addition to these core modules, Signifyd also provides specific solutions that leverage network intelligence to fully eliminate the need for merchants to manage common use cases themselves:

Fraud Prevention machine learning models contextualize insights from the Commerce Network with merchant- and vertical-specific data to block fraudulent orders while streamlining order fulfillment for legitimate customers. The solution includes two products: **Automated Recommendations**, in which orders are decisioned in real-time by **Signifyd**; and **Guaranteed Fraud Protection**, which pairs order automation with a financial guarantee against fraudulent chargebacks on all approved orders.

Abuse Prevention combines the underlying platform components (Commerce Network, Decision Center, Insights Reporting) with active monitoring and investigations of consumer chargebacks and proactive consulting on best practices for business processes and policies.

- **Policy Protection** allows merchants to build custom policies for common use cases such as promotion abuse and unauthorized resellers. Because the product gives merchants access to the Decision Center module, risk management teams are fully equipped to build, test, deploy and manage policies with functionality like policy simulation, lists, fulfillment and review workflow integration and more.

Signifyd

- **Return Abuse Prevention** allows merchants to streamline customer interactions and automate the returns process.
- **Guaranteed INR Protection** offers a financial guarantee against orders that result in an INR claim
- **Chargeback Recovery** integrates chargeback data directly via the payment gateways, allowing Signifyd to dispute consumer abuse chargebacks automatically.

This enables a closed-loop approach to prevent future abuse without putting unwelcome friction into the shopping experience for valid customers—even for those who file legitimate chargebacks.

Account Protection analyzes behavioral and device data from account login through checkout to defend customer accounts—and the sensitive financial information, gift card details, and loyalty points they contain—from malicious schemes and to mitigate damages posed to brand reputation. The solution includes the **ATO Protection** product which monitors consumer behavior across the Commerce Network to build a constantly evolving profile of each shopper within the network. These insights can be leveraged by merchants to build custom **ATO protection** at login while also allowing **Signifyd** to accurately detect anomalies in purchasing behavior and stop fraudulent orders as a result of ATO at checkout.

Payment Optimization combines the underlying platform components with a fully 3D-Secure 2.2 compliant interface to take advantage of exemptions and provide delegated, seamless strong customer authentication (SCA) as mandated by PSD2 in Europe. The solution includes two products: first, **Auth Rate Optimization** enriches orders sent out for authorization with data from the CommerceNetwork, giving banks the confidence to authorize orders that otherwise would have been falsely declined. Second, **SCA Exemption Management** intelligently analyzes incoming orders to surface thoseeligible for SCA exemptions, while ensuring minimal disruption for in-scope SCA payments.

Technical Integration

Clients can integrate via plugin or application programming interface (API). **Signifyd** offers plugins or is natively embedded in platforms such as Adobe Commerce Cloud (Magento), BigCommerce, Miva, SAP, Salesforce Commerce Cloud, and Shopify.

Direct API integrations require approximately three days' worth of development and testing. There are contractual service level agreements for system uptime, in addition to the redundancy that comes with hosting the system on the cloud platform Amazon Web Services.

Professional Services

Customer Success includes a dedicated customer success manager as well as unlimited support cases. Based on merchant needs, **Signifyd** offers ecommerce consulting provided by experts with specific commerce vertical domain experience. Common areas for consulting services include benchmarking, process optimization, and customer experience enhancements.

In development over the next 12 months:

Upcoming releases are scheduled for all components on a regular basis and will include further enhancements to capabilities, integrations, user interfaces, and models.

SpyCloud

SpyCloud Identity Risk Engine is an API-delivered solution that provides enterprises with actionable, predictive fraud risk scores for customers based on data that has been recaptured from the criminal underground. **SpyCloud** collects and analyzes billions of data points exposed in breaches and malware infections and correlates them across a customer's multiple online personas to produce a single, comprehensive risk signal.

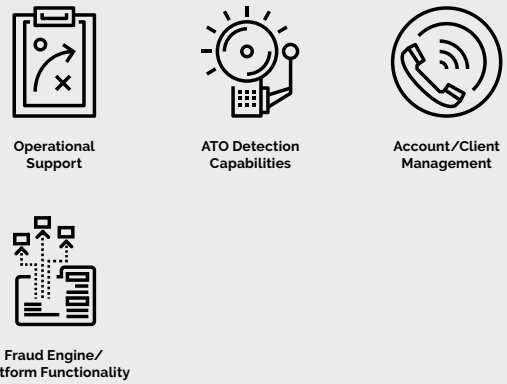
This data correlation provides unique insights that allow fraud teams to tailor the customer experience based on each user's risk level. Low-risk customers can transact friction-free, while medium- and high-risk users can be escalated for additional identity verification or blocked from transacting.

Solution

SpyCloud Identity Risk Engine provides ecommerce and financial services companies with a risk signal for each of their customers, derived from insights and historical recaptured underground data missing from other anti-fraud or identity verification solutions on the market. It offers actionable, predictive fraud risk assessments based on breach data, information siphoned from malware-infected devices, and other forms of underground data recaptured from criminal communities using human intelligence (HUMINT). **SpyCloud** leverages a proprietary engine that curates, analyzes, and enriches this data with threat context–delivering a single, risk score for each user alongside up to 20 reason codes and comprehensive supporting metadata. The service is designed to give customers an option to rely on the risk score and can further align their business needs by using reason codes and metadata as a way to customize their risk tolerance.

SpyCloud

At a Glance:



SpyCloud

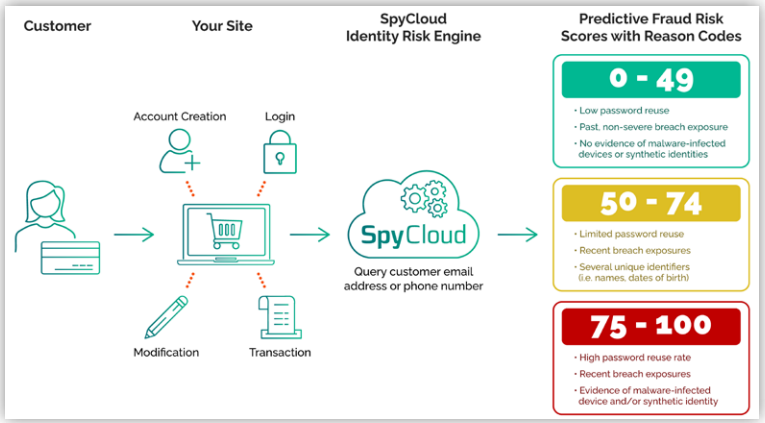
While most people have had some data exposed on the criminal underground, the fraud risk posed by that exposure varies substantially by the type of data exposed, the recency, and the method of compromise. The scores delivered by **SpyCloud** Identity Risk Engine correlate a user's multiple online personas and their associated exposures in data breaches, combo lists, or malware infections. Based on SpyCloud's assessment of the risk posed by users' exposed data, enterprises can identify and block fraudulent transactions without introducing friction for low-risk users.

SpyCloud enhances the power of existing fraud prevention and user authentication solutions by drawing on a continuously-updated database of over 145B+ recaptured assets from the criminal underground to illuminate customers' risk of account takeover, new account fraud, synthetic identity, and other forms of online fraud. By distilling billions of disparate data points into an API-delivered signal accompanied by key risk indicators, **SpyCloud** helps retailers and financial institutions make confident fraud decisions in real time.

Examples of Key Risk Indicators that comprise a user's underground exposure include:

- **Type of exposure:** i.e. third-party breach, combo list, or malware device infection
- **Breach recency:** how many days since the user appeared in a data breach or logs from a malware-infected device
- **Password reuse:** percentage representing the propensity of a user to reuse passwords across multiple exposed accounts
- **Exposure severity:** the types and amount of sensitive information/PII available to criminals

This is all achieved while maintaining the customer's data privacy.



SpyCloud Identity Risk Engine can be used where it is most impactful to the enterprise and can be called at the greatest points of account weakness (the points most susceptible to fraud) such as:

- Account Creation/account opening/account enrollment
- Login
- Account Modifications
- Transaction (including guest checkout)

SpyCloud

Primary Capabilities include:

- Reduction in the need for additional resources or time spent on unnecessary manual reviews
- Improved rates of fraud detection, resulting in fewer false positives, and potential for streamlined customer experience
- Aggregated data distilled into an underground risk score (with supporting key risk indicators) that acts as a signal for real-time decisioning
- Historical evidence linking exposed data, credentials, security hygiene, and other critical factors to help expedite fraud decisions and decrease the need for manual review
- Access to data drawn from sources that can't be found via web search, including breach data and logs from malware that allow bad actors to impersonate real customers

The SpyCloud platform can help support the following strategies:

- **Strengthening of Security Posture:** Positioning **SpyCloud** Identity Risk Engine at vulnerable points can help reveal risk, but can also offer insights into malware-stolen data criminals can utilize, including IP addresses and device IDs that are historically difficult to detect.
- **Forecasting of Targeted Attacks:** Real-time recaptured data helps identify customers with newly exposed credentials that are of high value to criminals.
- **Prediction of Fraud Tied to Malware:** Identify customers whose data has been harvested by malware, including browser fingerprints that enable criminals to impersonate them.
- **Anticipation of Account Takeover:** Determine which customers are at the highest risk of account takeover due to exposed credentials, bad password hygiene, and other key risk indicators.
- **Detection of Synthetic Identities:** Detect anomalies within a user's information indicating that the identity is fake, stolen, or constructed using sensitive data available on the criminal underground.
- **Defense Against Account Enrollment Fraud:** By linking billions of data points, SpyCloud identifies when pirated information from multiple exposures has been combined to create an unverifiable identity.

Proof-of-Concept (POC) process:

The POC process provides the ability to test data against historical data sets with known outcomes. This makes it possible to review the efficacy of the service and bring context to the ROI, including the ability to run the queries based on the date of the transaction. This gives the client an accurate reference of the "what if" data test. The pricing is an annual tiered volume transaction-based model.

SpyCloud

Channels of specialization:

- **B2B:** Selling directly to enterprises, particularly in ecommerce and financial services
- **Business Development Partnerships:** Seeking integrations with major fraud platforms/payment processors
- **Verticals:** Financial services and ecommerce industries

Integration

SpyCloud offers access to Identity Risk Engine via a high-volume, REST-based API, as well as via batch transmission. The API delivers sub-second response times and requires minimal effort to integrate, providing numeric and text character results for ease of ingestion. Access is also available via a growing number of partnerships and white label options. Support to active customers is provided without a separate package or cost. Integration guides are available and accessible by authorized users. The product information includes an interactive form to test individual queries.

12-month roadmap:

- **SpyCloud** Identity Risk Engine launched in January 2022
- Plans include several initiatives to help broaden **SpyCloud's** presence in different markets
- Customer-focused input will help drive some of the developments

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.

Experian

In October 2013, **Experian** purchased 41st Parameter, a fraud prevention company founded in 2004. With the purchase, **Experian** added device intelligence capability and rules engine expertise to its portfolio of fraud prevention and identity verification solutions.

Experian is now launching **CrossCore**, an open-ended platform allowing merchants to incorporate their own proprietary data and other third-party solutions, as well as core **Experian** products and services such as their identity verification and risk-decisioning platform, **Precise ID** and **FraudNet**. Both platforms will remain core components of the fraud prevention technology suite, while **CrossCore** acts as the flexible ecosystem to incorporate all other sources of data.

FraudNet is comprised of four core components:

- **Device Intelligence**
- **Rules Engine**
- **Investigator Workbench** (case management)
- **Link Analysis**

Experian is partnering with IQOR (a chargeback management company) to provide feeds directly into **FraudNet** via **CrossCore**. This data will be used to enhance model performance and will be incorporated into negative files.

At a Glance:

Experian 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

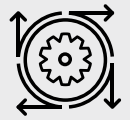
Feedzai attempts to provide a machine-learning-based fraud platform to help risk professionals do the work of data scientists using a guided, self-contained environment. Through **Feedzai DS**, teams are provided with a way to create advanced machine-learning fraud models. With extraction of features, 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:



Machine Learning

Fraud Engine/ Platform Functionality

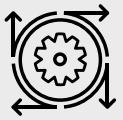
Feedzai chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

IdentityMind

IdentityMind's eDNA technology identifies the user behind every transaction and account activity. The platform then constructs a visual map of each identity, including the user's name, email, IP geolocation, user accounts, and 46 other factors.

As the user conducts transactions, the platform develops reputations for each user, and all the entities associated with them. These reputations are combined with a fully configurable rule set and policies to prevent fraudulent transactions. Merchants can use a large number of tools to increase the effectiveness of their anti-fraud policies, including worldwide identity verifications. Merchants can benefit from fraud and risk management information shared across **IdentityMind Global's** diverse network of banks, money services businesses (MSBs), merchants, and more.

At a Glance:



Machine Learning

IdentityMind 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.

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 every fraud detection technology available. **NoFraud** focuses on eliminating all fraud-related overhead and required expertise from its customers. They increase customers' approval rates and eliminate their chargeback liability through a combination of machine-learning technology and human intelligence.

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.

NOFRAUD

At a Glance:

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.

NoFraud

Chargeback Protection: NoFraud offers a chargeback guarantee and will reimburse the customer for fraud chargebacks that occured on transactions it accepted. In addition, **NoFraud** will dispute the chargeback on the merchant's behalf. **NoFraud** does not require any long-term contracts or commitments for its service.

Radial

Much like Magento on the web platform side, **Radial** is a spinoff service of eBay enterprise (formerly GSI commerce). At one point, the services were bundled, but have now been split into independent entities for a cafeteria-style selection approach.

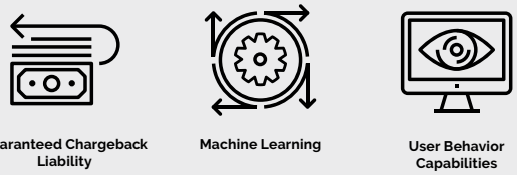
They offer a fully outsourced fraud solution, which includes a chargeback guarantee. While a full Application Programming Interface (API) integration is preferred, they do offer segmentation services like peak-season overflow volume and extreme high-risk products such as gift certificates. There's also a merchant portal available for one-off verification requests. Pricing is transactional and based on volume.

Benefits include:

- A single, central integration point for payment needs
- End-to-end fraud management
- Simple integration with several popular web platforms like Magento
- Zero fraud liability

Radial

At a Glance:



Radial 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.

Simility

Simility combines data, machine learning, and people to fight fraud. They utilize beacons, application program interfaces (APIs), and software development kits (SDKs) to generate data directly from a merchant's website and/or mobile app. This allows them to collect and transform merchant specific data feeds from varying sources directly into their interfaces. They can take structured or unstructured data, structure it to feed into their models, determine relations between the data points, and model it in flexible graphs showing objects and relationships.

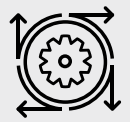
When information is added, their models will adapt and evolve to those patterns. They say the models adapt and detect patterns of fraud before they are perceptible to human analysis. Also, manual rules are arranged into code and fed into their machine-learning models.

They offer a user interface which is displayed in a singular view so analysts can visualize machine learning, manual rules, behavioral analytics, and device fingerprinting. This purportedly allows an analyst the ability to "slice and dice" the information to identify patterns and relationships.

Their solution has been engineered so merchants are not required to have their technical teams "write code." Their solution utilizes:

- **Device Recon:** Identifies devices by their fingerprints (characteristics and behaviors) and uses clustered proprietary algorithms to detect fraud.
- **Augmented Analytics:** Feeds manual rule-building directly into the machine-learning engine, which detects patterns to be implemented into the manual rule-builder.
- **Workbench:** Allows analysts to customize their workflows through a user interface that lets them automate their own work.

At a Glance:



Machine Learning

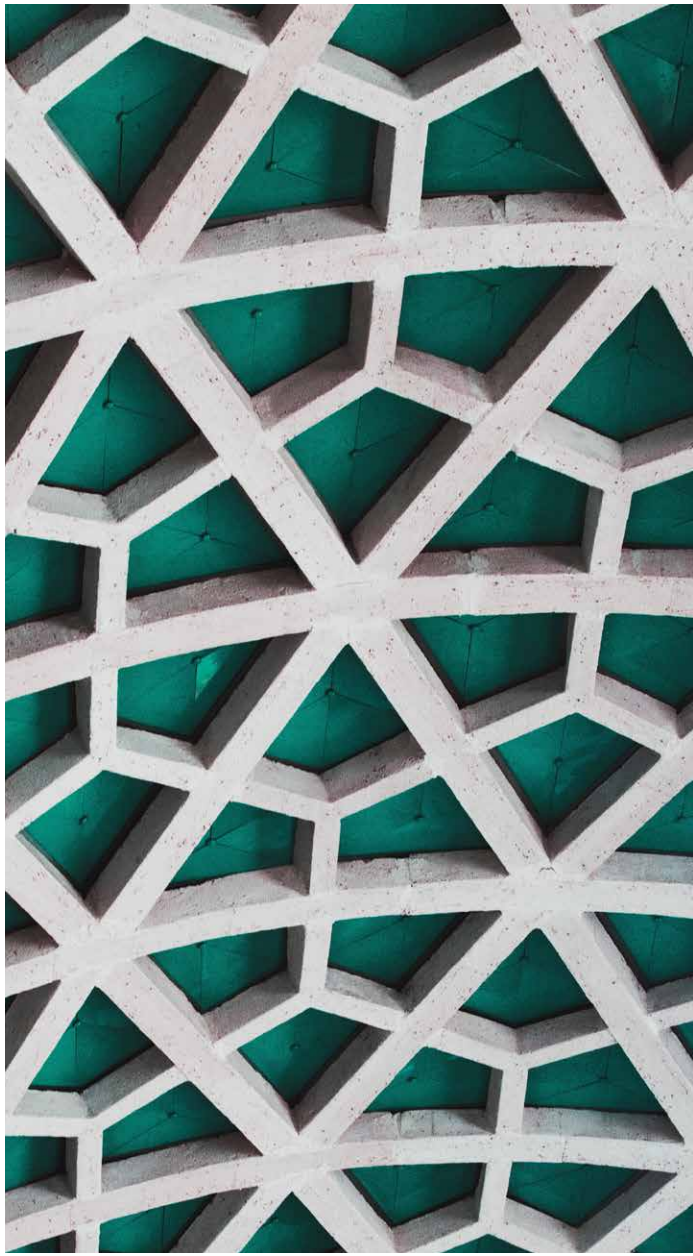
Fraud Engine/ Platform Functionality

Device Fingerprint Capabilities

Simility 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.



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:

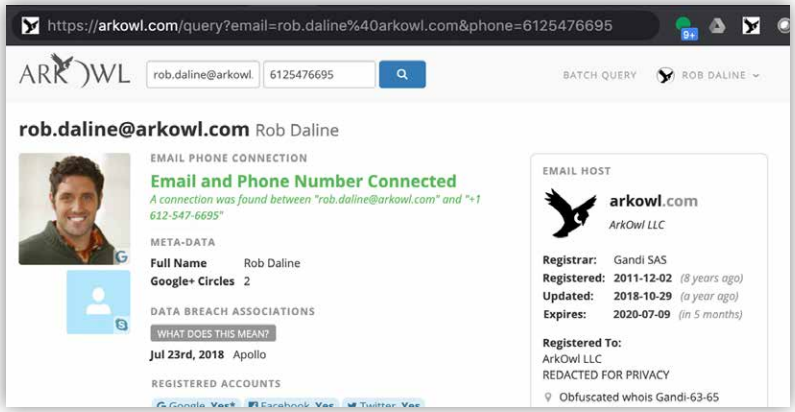
3rd Party API Capabilities

Professional Guidance/Services

Pre-Authorization Functionality

ArkOwl

In the past, the **ArkOwl** service has been limited to reverse email address lookups. However, with the latest version they have added real-time phone number verification to the email address data set already available. In the last year, they have added phone number verification, additional social media data, and European servers for **ArkOwl** data to be accessed through.



Reporting:

Options include history of email address or phone number, queried with in their system as well as analyst usage activity, with the ability to pull patterns as far back as two weeks.

Service / Support:

ArkOwl offers a free, no-risk/no-commitment "test drive," which can help generate valuable insights. (For example, orders using a customer email address linked with a Pinterest and Google account are 10 times less likely to be seen as fraud than the average order–and this insight can affect as many as 20 percent of orders surveyed. And, as a second example, in another instance, orders were 14 times less likely to be seen as fraud if the customer phone number and customer email address were linked—an insight that affected 36 percent of orders surveyed.)

Testing and analysis designed to support rule generation is available upon request. For proof-of-concept purposes, historical data analysis is available on both confirmed chargeback as well as valid order data. This can help provide insights into how decisions could or would have been made if the solution had been in place.

Users and Pricing:

There are no limits to the number of users per paid account. Available pricing plans include a monthly subscription, or pre-purchase queries and pay as you go. Payment methods accepted include credit card, check, or ACH. Customers can back out of contracts or return query credits at any time if the service is no longer satisfactory.

Integration:

Current time from signature to go-live is immediate, with average response times of .5 seconds. User Teams get an API key and/or direct web portal access. API integration documents and integration guides can be found here.

A manager account is created for user management purposes.

ArkOwl

This account allows for the addition of users, billing management, tracking of stats, and payments. Control management is maintained through permission based rule changes.

Existing third-party platform integrations include Accertify and Nice-Actimize, through which ArkOwl can provide data elements for writing and managing rules.

Near-future road map:

- Fraud risk score
- Increased phone and email address data sources

Emailage

Emailage, founded in 2012 in Chandler, Arizona, 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 Intelligent 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.

Currently, **Emailage** reports 78 percent of clients integrated directly and another 22 percent with indirect integration. They process more than one billion transactions annually—a number that has grown more than 50 percent year over year, according to the company.

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

Machine Learning

Professional Guidance/Services

Emailage

Solutions & Functionality

Emailage provides predictive risk scoring to detect fraud and deliver quality consumer experiences. Their new flagship offering, **Digital Identity Score**, launched in 2019, takes in a set of transaction attributes, leverages over 150 additional dynamic data points, and uses advanced machine-learning algorithms as the basis of transactional risk assessment. Core risk models are built around feedback from the network that provides actual transaction outcomes, updated on a continuous basis. Models can be customized for industry and individual company levels.

Digital Identity Score provides a set of scores and a detailed set of attributes around the risk of each transaction to aid in expediting approvals, preventing chargebacks, automating workflows, and optimizing the manual review process.

Digital Identity Score can be delivered via a standard API, or, for organizations requiring very high speed response, the **Rapid Risk** API is available. **Rapid Risk** API delivery response times are under 50ms.

Emailage Portal 3 provides the risk decisioning intelligence of **Digital Identity Score** in a web-based manual investigation environment. The system can be integrated with other environments using Single-Sign-On (SSO). A "deep-linking" option allows queries to be prefilled with relevant search data, creating efficiency and accuracy for users by eliminating re-keying errors. **Portal 3** users are able to upload data files for batch processing. **Portal 3** can be accessed via a browser plug-in, further streamlining the manual review process.

Portal 3 serves as the main hub for the following functions:

- Manually run **Digital Identity Score**
- Upload and receive batch data files
- Review recent transactions
- Find all necessary API and SFTP documentation
- View performance dashboards and run reports
- Manage queued jobs
- Review fraud warnings

Emailage in-house data scientists monitor the latest fraud trends, patterns, behaviors, and events to continuously refine and calibrate models. As a result, they have developed targeted fraud prevention solutions for several industries to outsmart their unique fraud types. Those verticals include:

- Ecommerce & retail
- Finance & banking
- Travel & entertainment

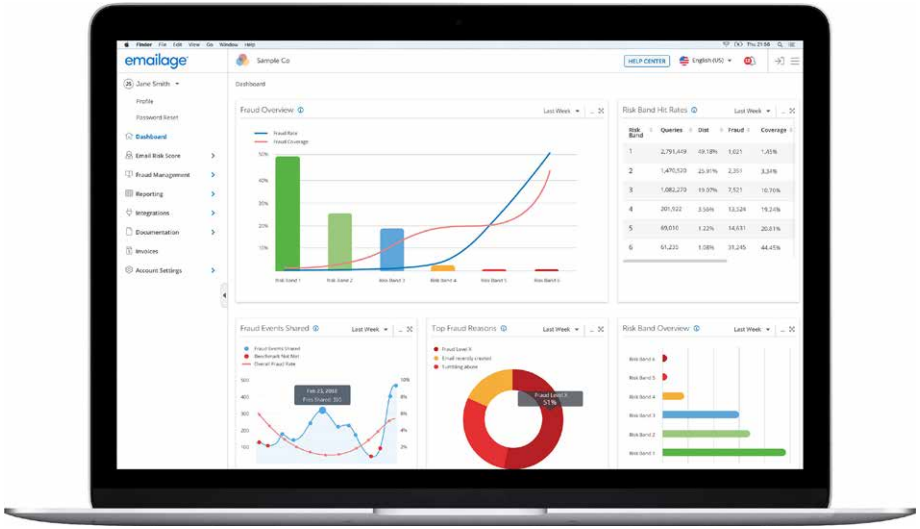
Emailage

- Technology
- Gaming
- Event ticketing
- Lending

Emailage clients benefit from access to a consortium model, which allows companies across the globe to collaborate in their anti-fraud efforts. Clients communicate the outcomes of transactions to **Emailage** through API, SFTP, or batch upload. As feedback is shared, the machine-learning algorithms become better at predicting and adjusting to industry- and company-specific fraud patterns. There is no incremental cost, nor does this constitute opting in.

As clients begin to pass data fields to **Emailage** and share fraudulent events, machine-learning algorithms detect patterns and trends; this creates the opportunity to further calibrate and refine models around those trends. Ongoing refinements affect the overall score of a transaction, pushing the resulting score away from the center risk bands and toward low-risk or high-risk bands—auto-approve or manual review, respectively.

The size of their client base has allowed **Emailage** to grow into a global intelligence network with instant access to fraud signals associated with nearly one billion unique email addresses connected to IP addresses, domain names, phone numbers, and more. Positive signals from these elements can help merchants approve more customers and prevent more fraud.



Reporting and UI

A full set of reports and dashboards is accessed via the **Emailage Portal 3**. Custom reporting is available through a client's Customer Success Manager, who works to understand their needs and design the appropriate report.

Portal 3, launched in 2019, provides clients more robust reporting access, including dashboards displaying risk band distribution, fraud hit rates, and coverage rates—as well as other valuable details to enable optimization of the platform.

Emailage

Services Offered

Emailage partners with clients from Proof of Value (POV) validation to installation and offers on-going support. The fraud strategy team provides a comprehensive review to optimize performance. This service ensures maximum value in fraud prediction and improved customer experience. A team of Customer Success Managers work closely with clients beginning with installation.

Clients who share transaction outcomes receive custom scoring calibration, including industry-specific modeling. Working with our team of experienced data scientists, **Emailage** clients typically see significant increases in efficiency and fraud capture rates when they provide outcome data.

Integration Options

Emailage has the ability to run a Proof Of Value (POV) using retrospective analysis on historical transactions or live data. During the POV process, clients have access to a dedicated Customer Success Manager and data science experts who collaborate with clients to analyze and optimize models for maximum performance.

Options for integration include the standard API, the Rapid Risk API, SFTP (Secure File Transfer Protocol), **Portal 3**, and extensions for Chrome and Firefox browsers. **Emailage** partners with a number of existing platforms including Accertify, CyberSource, Equifax, Experian, and LexisNexis Risk Solutions, among others. Integration guides are available and easily accessed via the client portal. All documentation is available upon signing of an NDA.

Emailage solutions set up via a partner platform are typically completed within 24 hours of signing a contract. If a client decides to utilize direct integration options, the setup is accomplished via fully documented API. **Emailage** offers the **Query Explorer** tool to instantly generate the code necessary to make API calls, streamlining integration.

Response times are measured as the time taken to process a transaction. Using the standard API, 99 percent of responses are returned in less than 950 milliseconds. The measurement is taken over a rolling 30-day average, excluding WAN network latency. For clients who need faster response times, the **Rapid Risk** API offers response times below 30 milliseconds, and is able to process up to 400 transactions per second, to effectively support risk decisioning at scale.

Live, up-to-the-minute information on service levels and any network interruption notifications can be found through their status link at status.emailage.com.

Emailage

Pricing

Emailage uses a subscription-style pricing model with a minimum subscription of 5,000 queries per month. Client-specific pricing is adjusted based on the length of the agreement and committed query volume. **Portal 3** is offered via seat license, allowing unlimited manual input queries for a fixed price on a per-user basis.

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 uniquely identify site visitors and app users in multiple environments including MAID-less and third-party cookie-less.

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.

For the media ecosystem, **Intent IQ's** identity resolution solutions facilitate clients' cross-app, cross-site, and cross-device targeting and attribution. This is done both accurately and on a large scale.

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

Professional Guidance/Services

Pre-Authorization Functionality

ATO Detection Capabilities

Intent IQ

Intent IQ's philosophy is that its biggest advantage is knowing the real person, their household members, and their devices. The fraudster does not.

The **Intent IQ** assembled knowledge can be masked but not directly re-created, for different reasons, including that most of that knowledge is not known to the fraudster. Such knowledge includes the real person's home IP addresses (including historical IP addresses), devices including their email and log-in activity, and internet providers. These (amongst other) elements are matched real-time and tracked as they change. The details can be accessed real-time via APi or via Batch file.

As **Intent IQ** continues to expand into new markets and verticals, they are utilizing the tested approach of powering platforms that serve end-clients. They're increasing focus on companies serving financial institutions and specializing in account take-over and new account fraud.

Intent IQ operates by using two **methods of integration:**

- Via an online HTTPS API
- Via an offline file Amazon S3 bucket (incoming folder for input and outgoing for output)

Their proof of concept includes a process whereby a potential client sends a log file made up of historical login events from the previous six to nine months. These login events include both authenticated users and users who turned out to be fraudsters.

The file includes the following requested data fields:

- Time/date of login
- IP
- User agent
- Email address in hashed format
- Latitude/longitude of the person's household postal address

Intent IQ will analyze the log file and provide the prospect with perceived fraud attempts based on any mismatch between the real person and their household devices and the user attempting to log in.

Once integrated, the following client support options are offered:

- Ticketing system
- 24/7 slack channel response
- Emergency help desk/phone support
- Bi-weekly tech support
- A dedicated Customer Success manager

Intent IQ strives to align its business success with its clients' success. In keeping with this philosophy, pricing is flexible. Monthly minimums are put in place to protect some of **Intent IQ's** resource investment in the partnership.

Intent IQ

Key developments over the past 12 months.

In the last year, Intent IQ made the following announcements:

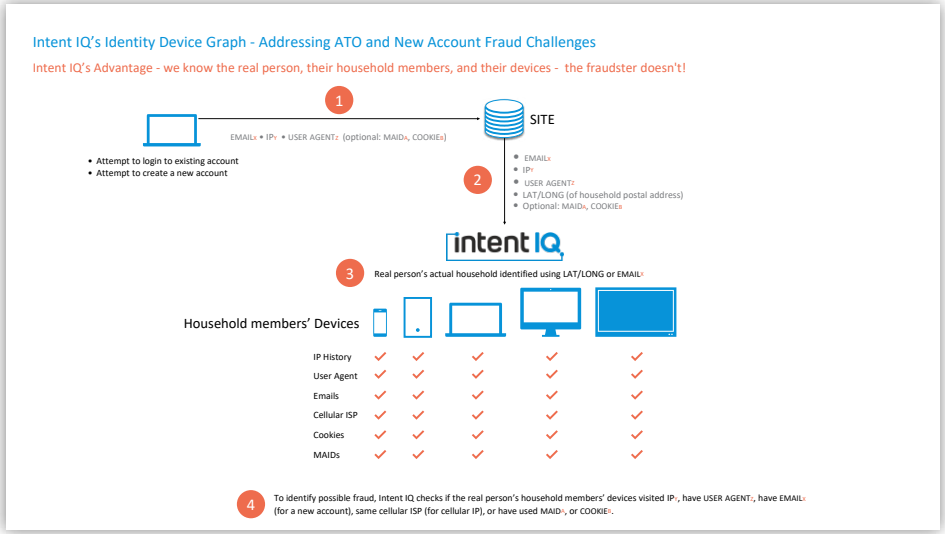
- **Intent IQ** introduced Mobile Identity Hub ('MIH'), its ID solution for MAID-less environments, such as the one created by IDFA deprecation or AAID future elimination, by stepping-in and providing a privacy friendly universal ID that facilitates cross-app targeting and attribution. **Intent IQ's** solution is in line with the online advertising industry standards and in compliance with the law (incl. CCPA). Originating from the people that invented and evangelized AdChoices, privacy is in Intent IQ's DNA.

  MIH leverages **Intent IQ's** experience in providing accurate and scalable solutions to cookie-less environments.

- A patent-pending cross-app attribution solution, ATTLICA™. When a client's IDFA-less data is assigned to a device by **Intent IQ**, the data is immediately turned into aggregated data, to avoid device-specific cross-app attribution. This aligns with Apple's App Store privacy and data use practices. However, unlike SKAdNetwork, **Intent IQ** is able to provide the same granular attribution post-iOS 14, in scale and with the same accuracy as pre-iOS 14, along with a months-long attribution time window.

12-month roadmap

In the coming year, **Intent IQ's** ability to identify a device using only an IP address and the user agent originating from the device will become more important than ever. Validating device user-claimed credentials will be crucial given Apple's deprecation of IDFA and Google's expected elimination of third-party cookies in early 2022, combined with browsers expanding blockage of device fingerprinting.



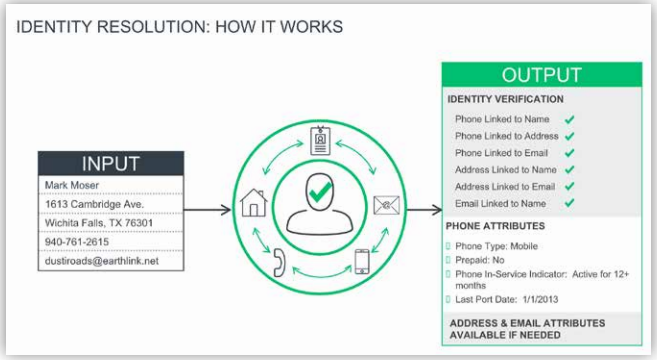
Neustar

Neustar, a Transunion Company, helps companies efficiently connect with customers while mitigating their fraud and compliance risk. **Neustar** fraud and authentication solutions provide the "unspoofable" consumer insights needed to know with certainty who is at the end of every interaction, creating trusted and frictionless consumer interactions.

Neustar leverages an authoritative network of physical, digital, and device identity data, in addition to other signals, like browsing footprint. They allow companies to let legitimate customers through faster, while flagging risky transactions for additional verification, in both digital and call center environments. Key performance indicators (KPIs) of focus include chargeback rate, manual review rates, operational efficiency (IVR/contact center), right-party contact rates, false positive rates, revenue-per-dial, average call handle time, lifetime customer retention, and customer satisfaction.

Solutions and Functionality

To **Neustar**, "identity resolution" means using a host of authoritative identity signals to quickly identify, authenticate, and fast-track legitimate customers and interactions while mitigating against the negative impact of fraud. The more accurately consumers can be identified, the harder it is for malicious users to spoof identities and take over accounts. It ultimately makes better decision-making possible, along with a more frictionless consumer experience. **Neustar** works with and provides identity intelligence to the top 10 leading banks, the top 10 leading card issuers in the U.S., and some of the biggest brands across every industry and vertical.



neustar®

At a Glance:

- 3rd Party API Capabilities
- Machine Learning
- Guaranteed Chargeback Liability
- Account/Client Management
- User Behavior Capabilities
- Pre-Authorization Functionality
- Fraud Engine/ Platform Functionality

Neustar

This is achieved through the **Neustar OneID** system—a repository of online and offline data that is broken down, corroborated, and rebuilt up to every 15 minutes with updates from sources with direct relationships, including billing, telecom, and government agencies. **Neustar OneID** is powered by an always-on network of partners, many who are the provisioning source, who provide constantly updated consumer attributes and identity linkages, both online and offline. They then overlay proprietary attributes about phone behavior and develop a wide range of fraud solutions.

This larger view of identity serves as a foundation supporting other primary products and services. The identity platform is used by entities focused on fraud, compliance, and operational efficiency/ customer experience. It allows insights into phone number ownership and attributes. And it also offers deep intelligence into IP reputation, synthetic consumer names in the carrier ecosystem, anomalous phone number movement between carriers, mobile device behavior, and a host of other intelligence data points.

As fraudsters have begun to manipulate phone carriers with softer controls, malicious users are taking advantage of these vulnerabilities to commit identity fraud. **Neustar** has recognized this attack vector and developed a phone reputation score that helps users identify the potential of such an attack.

These technologies are applied in a number of ways, by a number of organizations, across verticals and industries. They allow Neustar to help users focus on mitigating reputational harm, financial impact, and negative customer experience.

There are four primary product offerings:

Account Origination Fraud

Digital Identity Risk uses a wide range of online, offline, and device-based intelligence to separate legitimate users from fraudsters. **Neustar** uses a host of elements, including IP, browsing, phone activity, and connections to digital footprints of a person or household. With these elements, they corroborate the digital information against offline consumer data and provide organizations' decisioning engines with additional, differentiated data that can help indicate the trustworthiness of the digital identity. Predictive scores based on machine-learning models provide easy-to-understand signals for fraud mitigation.

Neustar

This digital authentication concept has been expanded to further help understand the person behind every transaction. This means both heightened levels of risk mitigation as well as further reductions of inadvertent rejection or step-up requirements of legitimate users.

The evolution of **Digital Identity Risk** provides clients with a few distinct options:

- **Pro Level** combines a wide range of intelligence about users, including device, IP history, characteristics over time, advertising and publishing key signals, what websites this device has visited, and indicators of potential threats.
- **Flex Level** extends the reach of clients with fewer integration and data science resources for quick and simple implementation. It utilizes fewer signals, which are more easily consumed, while allowing users to add data elements over time.
- In addition, a recently added **Device Fingerprinting** functionality can tie together consumer behavior and location. This provides enhanced ability to verify the identity behind the device.

Account Takeover Fraud

Phone Takeover Risk helps organizations ensure that their outbound texts and calls reach the intended consumer and not a fraudster. For contact centers that make large volumes of outbound consumer calls or one-time passcode texts, authenticating the user's identity on the other end of the number in real-time can be difficult. The result is that fraudsters may intercept two-factor authentication calls or texts to commit account takeover fraud. Using Phone Takeover Risk, Neustar can help identify phone numbers at high risk for fraud. They do so by addressing the three attack vectors below using near real-time data:

- **SIM Swap** helps to identify cases where a mobile phone number has recently become associated with a new SIM card. SIM-swapped phones are frequently used in account takeover attacks.
- **Call forwarding** allows users to confirm whether the number is being forwarded, and in many cases, to whom it's being forwarded. Because of the access to offline data (associated addresses), this service can confirm both high- and low-risk forwarding.
- **Unauthorized reassignment** can determine whether a phone has been reassigned from one carrier to another. It can identify the previous carrier, current carrier, and technology type. (For example, moving from mobile to landline, or from an AT&T number to a Google voice number). If **Neustar** identifies that reassignment has occurred, it will notify the client through their CRM database within two minutes of the event.

There are two primary ways to consume the service: via API request, or by onboarding phone numbers and continuously monitoring.

Neustar

Continuous monitoring is commonly used where financial, reputational, and regulatory risk are high.

Inbound Authentication: This solution, which leverages **TRUSTID** technology, identifies and authenticates inbound callers in near real-time, before the call center agent picks up the phone, even if the caller is using a phone number other than the one in their CRM record. The technology is especially helpful considering the rise in synthetic phone number use, as well as potentially spoofed or virtualized numbers.

For the 75 percent of callers using mobile phones and residential cable and landlines, **Neustar** Inbound Authentication confirms that the calling phone is engaged in a call with the call center through a real-time deterministic inspection of the call and calling device. Callers using common vectors of call center fraud are never authenticated. Callers that pass inspection experience significantly fewer KBA questions and can be trusted with higher-value options within an IVR.

For another 20 percent of calls, a live inspection of the calling device is not possible. Instead, Neustar Inbound Authentication leverages results from its history of inspecting billions of calls and additional data about calls, carriers, and network routing from its role as a licensed telephone carrier. The results allow for the stratification of caller treatment by trust level.

A small percentage of calls (three to five percent) may be sent for closer scrutiny, along with many of the signals that drove their probabilistic risk assessment scores. Call outcome results, shared via a client feedback community, continuously improve detection rates and reduce false-positive rates over time.

Neustar Inbound Authentication delivers more frequent and reliable "green" authentication by adapting uniquely to the caller's device, combining the coverage of probabilistic risk assessment with the accuracy of deterministic authentication. 95 percent of callers get streamlined service, more reasons to stay within the IVR, and faster resolution. The remaining callers get closer scrutiny to contain true positives for fraud—even on first-time attacks—and reduce future false positives.

Neustar Inbound Authentication reduces fraud risk, improves customer experience, speeds call resolution, and reduces IVR-to-agent transfers.

Target user groups include large inbound call centers, as well as financial, credit union, insurance, government, retail/ecommerce, healthcare, and utilities services. While customization options do exist, the out-of-the-box solution is robust enough for most applications. Integration includes a solutions architect and a customer success contact. Direct API integration can typically be achieved within a week, depending on the needs and setup of the client.

Neustar

TransUnion Acquisition

In late 2021, **TransUnion** acquired **Neustar**. Digital commerce continues to grow globally—and **TransUnion's** powerful digital identity assets, enhanced by **Neustar's** distinctive data and digital resolution capabilities, will make it possible for consumers and businesses to have safer and more personalized online experiences.

The combined businesses will provide enhanced fraud detection and prevention capabilities, using advanced data analytics and online identity behavior insights, to safeguard transactions across phone and digital channels to deliver superior consumer experiences. Customers will also benefit from debt recovery solutions distinctive to the market.

Services offered:

- **Neustar** client success teams include project management support. Clients may request custom models, which can add complexity and lengthen integration timeline.
- The typical pricing model is per query, but some applications (such as notification platforms and real-time port notifications) do require a monthly minimum.
- The **TransUnion** acquisition will accelerate development of the digital identity verification, device risk intelligence, and customer feedback data key to the **Neustar** fraud strategy and online identity graph.

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

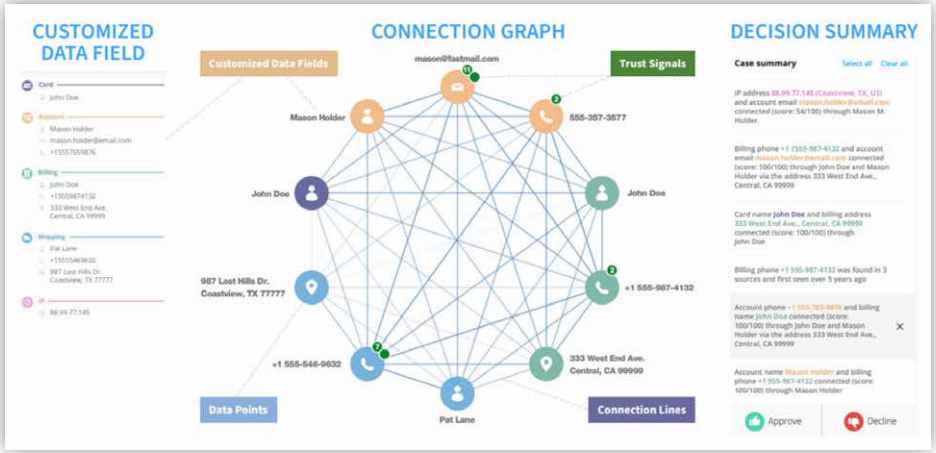
Pre-Authorization Functionality

Solutions & Functionality

Primary solution offerings fit into two distinct categories:

- **Pipl Trusted Intelligence:** Delivers instant visibility into the trust signals and connections behind data fragments to uncover trustworthy customers. Powered by **Pipl's** global index of nearly 4 billion online identities, Trusted Intelligence is the only solution that instantly displays data points that are connected, how they are connected, and which connections are meaningful to the transaction in question.

Key performance indicators (KPIs) of focus include: false declines, manual review times, and customer insult.

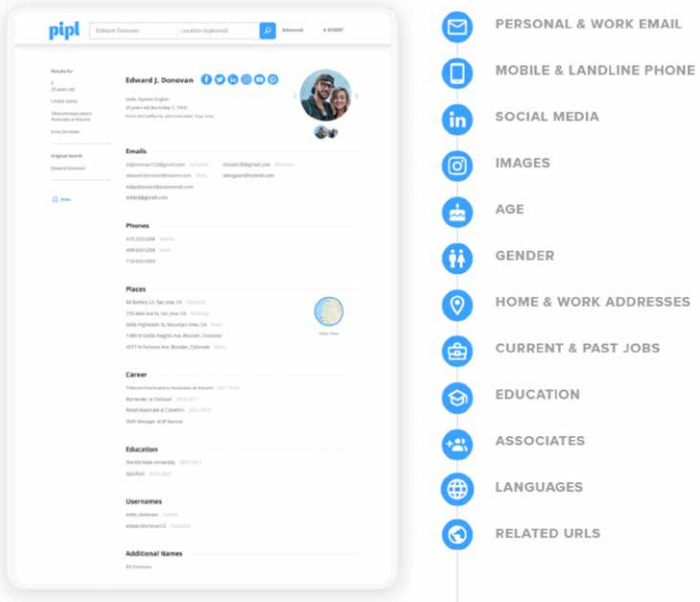


Pipl Trusted Intelligence

- **Pipl SEARCH:** Allows reviewers and analysts to quickly determine if a buyer is using a real identity and how that buyer may be connected to specific locations, emails, people and businesses. Conversely, it can help determine if the buyer is likely to be using false or synthetic identity information. This reduces manual review times across the entire fraud team. Key performance indicators (KPIs) of focus include: case time/ operational cost, case resolution rate, and verification accuracy.

To ensure a good merchant fit, an extensive proof-of-concept (POC) process exists for both Trusted Intelligence and SEARCH options.

- **Trusted Intelligence:** To ensure success, a dedicated solutions engineer performs a data evaluation plan for the customer at no charge. After integrating **Trusted Intelligence** into their test environment, customers have access to robust identity trust information as well as source and timestamp metadata that provides a historical record of the identity.
- **SEARCH:** The process includes a pre-POC evaluation session, analyst onboarding and training, an evaluation period for analyst teams, and a post-POC report with analysis. All of this is provided at no cost to the customer after speaking to their dedicated account manager.



Pipl SEARCH

Reporting

Pipl customers are assigned dedicated account management resources to help customize the reporting of SEARCH and Trusted Intelligence products based on the unique requirements of the customer. This may include metrics such as:

(through manual SEARCH function)

1. User query types and volumes with timestamps (by user)
2. Match rates
3. Email alerts for important updates and account information

(through Trusted Intelligence function)

1. Usage dashboard
2. Match rate information
3. Email alerts for important updates and account information

Pricing Format

Pricing for the two primary services are as follows:

- **SEARCH:** An annual license fee applies per user, with unlimited searches
- **Trusted Intelligence:** Transaction-based
- **Custom pricing and packaging options are also available:** contact Sales for additional pricing information

Integration Options

Integration options into **Pipl's** API can be found here. The RESTful API can be integrated using a choice of technologies (Python, C#/.NET, Java, Ruby, PHP). **Pipl's** code libraries are recommended.

Depending on a number of variables (sprint cycles, competence levels, team capacity, project prioritization, complexity of workflow, etc.), **Pipl's** API can integrate anywhere from a few hours to a few weeks. If already integrated with a channel partner, the process is greatly expedited and simply requires activation.

Support

All customers are provided dedicated customer success managers at no additional cost. **Pipl** offers both pre-POC and ongoing support through its team of solution engineers.

In the coming months:

While **Pipl** does not publish its roadmap, they are focused on the following features in the coming months:

- Enhancement of Trusted Intelligence APIs
- Launch of contributory network
- Continuous expansion and refinement of their massive data index

Socure

Socure's approach to identity verification and fraud prediction is predicated on the notion that, as consumers today lead increasingly digital lives, they leave breadcrumbs or "signals" about themselves both online and offline. For the new, digital-first paradigm in commerce, **Socure** provides a real-time, predictive analytics platform that combines the newest forms of machine learning and artificial intelligence with online and offline data. This allows the company to deliver the most accurate and broadest coverage for Know Your Customer (KYC) identity verification, AML/watchlist, and fraud prediction solutions in the U.S. market—at the Day Zero stage and throughout the user and identity lifecycle.

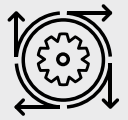
CEO Johnny Ayers co-founded **Socure** in 2012 after seeing first-hand how legacy incumbent solutions were unable to positively and accurately verify thin-file millennials and immigrants online when opening new accounts—while also predicting identity fraud and minimizing customer friction.

Today, **Socure** has an impressive client roster, including three of the top five banks, six of the top ten issuers, and many of the world's largest fintech, ecommerce, and payroll service providers. **Socure** helps these clients better assess identity risk, substantially increase auto-acceptance, reduce fraud losses, and optimize manual review/step-up verification for transactions and new applications across the digital ecosystem.

Socure leverages an abundance of authoritative data sources, including traditional and offline data, real-time data, and social data to generate over 3,000 predictive variables associated with email, phone, address, DOB, SSN, device, IP, name, and physical documents, among others. Internal and third-party data sources used include credit header, MNOs, DMVs, insurance companies, utilities, energy companies, and the open web. **Socure** also utilizes an in-house search capability as well as contributory

SOCURE

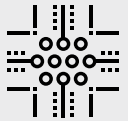
At a Glance:



Machine Learning

Device Fingerprint Capabilities

Pre-Authorization Functionality



Non-Production Real Time Rules Testing

and proprietary alert list databases in developing its machine-learning models.

Socure's fraud and identity solutions were designed and optimized to focus on the riskiest top 2% to 3% of applicants, drastically increasing fraud capture and reducing false positive rates in the most critical review and decline populations possible. Through this focus on accuracy, the company supports a number of use cases, both pre- and post-authorization—such as new account creation, sign-in, guest checkout, account update, and more. The company serves a wide market base where identity verification is particularly valuable, such as financial services, ecommerce, shared marketplaces, telecom, healthcare, insurance, and government.

Solutions & Functionality

The **Socure Sigma Fraud Suite** provides industry-specific machine-learning models that have been trained with their top 150 fraud predictors, using both good and fraud performance feedback from a network of the company's clients across industries. The **Sigma Fraud Suite** is optimized and monitored with live performance feedback data across the client base to ensure the highest accuracy levels possible and provide input to continuously improve model performance. The **Sigma Fraud Suite** is designed to capture multiple third-party and synthetic ID fraud types.

Socure's Email, Phone, and Address Risk Scores can be applied in a number of situations. Often, organizations wish to assess specific elements of an identity for further verification. This is especially true when the origination process is limited to a few identity attributes.

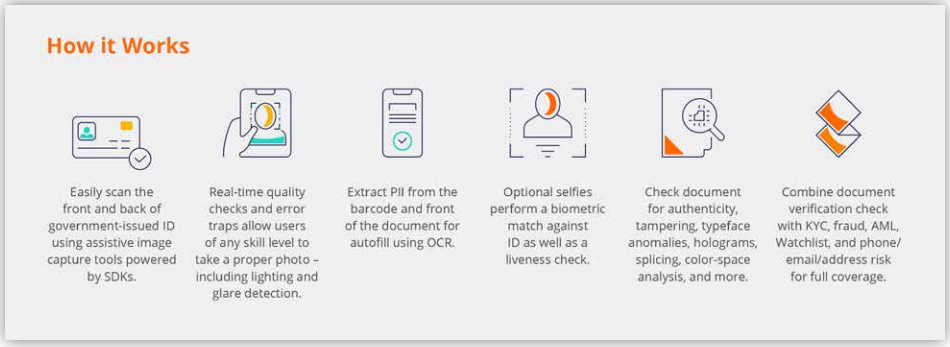
Their identity element-specific machine-learning models are trained with 50+ element-specific variables to predict the likelihood of fraud and risk by leveraging validity, correlation, age, risk, activity, and more. **Socure's** service has greater than 96% coverage for emails, phones, and addresses. In addition, **Socure's** device risk module verifies session authenticity by collecting unique features from a device or browser and allows a positive identification during subsequent visits. Device risk functionality can be utilized as part of a comprehensive identity verification solution.

KYC/CIP: Socure's Intelligent KYC provides the most complete identity coverage. Inclusive by design, it is the definitive outcome of advanced data strategies that identify people and amplify the voices of the most underserved demographics. **Socure** can help redesign and streamline the CIP process through large and inclusive datasets so that younger demographics, thin-file, credit invisible, and new-to-country applicants experience a more frictionless onboarding experience.

Socure Document Verification (DocV) is available via direct API as well as lightweight Mobile/Web SDKs (under 5MBs without

sacrificing features). **DocV** provides accurate primary or secondary physical document identity verification while also reducing the friction associated with knowledge-based authentication (KBA) approaches. **DocV** ensures that the document presented is authentic, and it then uniquely correlates the personally identifiable information (PII) elements presented in the application (Name/Address/DOB) to those captured from the document. A live selfie capture ensures that the user is submitting a document that belongs to them.

A more deterministic identification is achieved when **DocV** is used in conjunction with **Socure's ID+** to create the only 360˚ view on identity. This multidimensional approach layers on KYC, Global Watchlist, address verification, and email, phone, IP address, and device risk to provide a deep analysis—with the ability to capture even the best-falsified documents. Best-practice logic for decisioning is also provided based on performance feedback across **Socure's** customer base. **Socure's** products, including Document Verification, are available through a single API, and Mobile or Web SDKs. **DocV** is also the first document verification vendor in the world to provide phone, device, and document risk in a single, fully integrated solution.



Anti-Money Laundering (AML) Watchlists: Socure's AML Screening with Monitoring uniquely elevates identity resolution in AML frameworks to identify critical risks while leading the market in minimizing false positives. The solution helps companies identify whether they can do business with entities and what risks those entities bring. From Day Zero through the customer lifecycle, watchlist monitoring provides updates as risks are identified and then provides businesses with the intelligence to know when a risk is no longer relevant.

Alert List: A consortium database of over 150 million records of first- and third-party fraudulent identities, tagged per industry, utilizes **Socure's** extensive and cross-vertical client network. **Socure's** give-to-get model is updated weekly.

In order to ensure maximum performance, **Socure** is constantly creating new features (predictors) and fine-tuning its solutions. The proprietary and automation-first approach serves to develop highly predictive positive or negative correlated features that are then used in subsequent re-training of machine-learning models. This continued learning, driven by performance feedback data

across the network portfolio,serves as **Socure's** end-to-end machine-learning foundation for building, training, selecting, and deploying highly accurate models. **Socure's** machine-learning models are continuously challenged with updated models to determine if they can outperform current versions. This continuous, automated loop is what produces the most up-to-date and relevant fraud, correlation, and risk scores available in the market.

Unlike some consortium services, **Socure** does not simply collect and store positive and negative feedback data in a database. They take the next step of running statistical tests on the feedback data and using the results to continuously improve predictive models. They believe that the real value of feedback data is in how it is used to test data sources, develop highly predictive features, and re-train existing machine learning models to achieve superior performance.

Services and Integration

Socure offers a JSON response via a single RESTful API integration that's just four lines of code. Rather than providing raw data, they typically provide predictions that are actionable and highly accurate in solving specific problems.

In the case of more sophisticated organizations, responses can be "matrixed" or overlaid on top of their own existing ML models. This allows a customer to compare the two models to deliver the best and most accurate results possible. The approach also attempts to reduce the "accuracy problem" inherent with non-AI legacy rules engines.

Because there exists significant customer variability across industry segments and company size, a number of integration options for deployment are supported. Beyond the API integration, end-users can deploy the functionality through one of 18 integration partners. In the event a partner is used, the technical integration is already built within that platform. The third party would simply need to "turn it on" for the client. In this arrangement, the third-party platform would serve as an "orchestration engine." Through this connection, the client would be allowed to triangulate the details, which can deliver the best response possible. While the third-party platform serves as the orchestration point, all support functions come straight through **Socure.**

Pricing is generally transaction-based, with pre-set monthly minimums, a setup fee, and an annual license fee.

Vertical Markets

With a wide range of identity verification products, **Socure** has attracted customers in a number of verticals, including those in

the most stringent regulatory environments such as financial services. With a lightweight, digital native approach, it has gained market share with fintechs, including Chime, SoFi, Stash, and Varo. More recently, **Socure** has penetrated new verticals such as online gaming, working with a number of the top brands in this fast-growing industry. Other verticals with recent, notable wins include virtual care and the gig marketplace.

EKATA

Seattle-based **Ekata** provides global identity verification solutions via enterprise-grade APIs for automated decisioning, as well as **Pro Insight**, a SaaS solution for manual review. Ekata solutions help businesses reduce friction, improve conversions, and combat fraud. Their product suite provides accurate identity data and insights to reduce fraud and mitigate risk for companies around the globe.

Ekata's solutions provide data to businesses to help them:

- Detect fake account creation
- Conduct confident manual reviews
- Reduce payment risk

The data behind Ekata's solutions are powered by the Ekata Identity Engine, proprietary intellectual property that uses unique datasets from the **Ekata** Identity Graph and the **Ekata** Identity Network to provide identity verification data with consistent results across the globe, in industry-leading response times.

The **Ekata** Identity Engine comprises three elements:

- For more than two decades, **Ekata** has sourced data to build the **Identity Graph**. Across 100+ authoritative sources, they use data science to curate, corroborate, and connect the links between the digital (email and IP) and physical (person or business name, phone, and address) attributes for identity resolution in their graph.
- The **Ekata** proprietary **Identity Network** helps businesses identify good and bad customers in the act by analyzing patterns of how their information is being used in digital interactions using behavioral patterns and transaction-level intelligence from more than 400M monthly queries provided by **Ekata** customers.

At a Glance:

3rd Party API Capabilities

Machine Learning

Pre-Authorization Functionality

Ekata 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.

By integrating **GeoComply**, organizations are able to detect fraud earlier in a customer's engagement. This capability provides high performance fraud detection via the use of accurate, authentic, and unaltered location data acquired from a user's device.

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** - Use geolocation for better identity verification for KYC (know your customer) and enhanced due diligence, as well as for more confident automated underwriting.
- **Transactions Fraud Mitigation** - Require location checks to discourage bad actors and improve accuracy in differentiating between real fraud and false positives, as well as reducing false negatives.

GEOCOMPLY
Empowering The Future Of Digital Trust

At a Glance:

3rd Party API Capabilities

Account/Client Management

Device Fingerprint Capabilities

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.

GeoComply

- **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.

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:

API

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.

Nuance

Nuance Security Suite is an integrated multi-modal biometrics solution that helps organizations protect themselves and their customers across voice and digital channels.

Leading organizations around the world are addressing this problem with new technologies, including biometric security. With biometric security solutions, a customer can be authenticated using just their voice, face, or other biometric modalities. Fraudsters can be caught as they impersonate people.

Nuance fraud solutions find known and unknown fraudsters impersonating legitimate customers and stop criminal activities in customers' contact centers, mobile apps, and websites.

This fraud challenge is only poised to grow, with the increasing number of channels on which consumers engage and the rise of the digital wallet. Fraudsters do not approach account access in a siloed manner; instead, they take advantage of growing numbers of channels, devices, and access points. In order to truly combat fraud, organizations need to have a cross-channel security approach that stops fraudsters wherever and however they attack.

NUANCE®

At a Glance:

3rd Party API Capabilities

Machine Learning

Account/Client Management

Nuance 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.

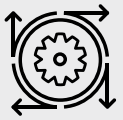
Onfido

Onfido helps companies see real identity—the humans behind the screens—using AI and identity experts. Customers can prove identities, wherever they are, with just an ID and their face. They can then re-verify or authenticate when needed with a selfie. Each response is classified as either "clear," "caution," or "suspected,." so fraud teams know exactly when to take action.

Traditionally, organizations have to rely on signals to trust a new user—for example, IP address, phone number, or credit database look-up. However, these signals can also be abused by fraudsters, which can create uncertainty.

Onfido Document Verification lets users scan a photo ID from any device and verifying that it's genuine. This, combined with Biometric Verification, can help create a seamless process for connecting an account to the real identity of a customer.

At a Glance:



Machine Learning

ATO Detection Capabilities

Onfido 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

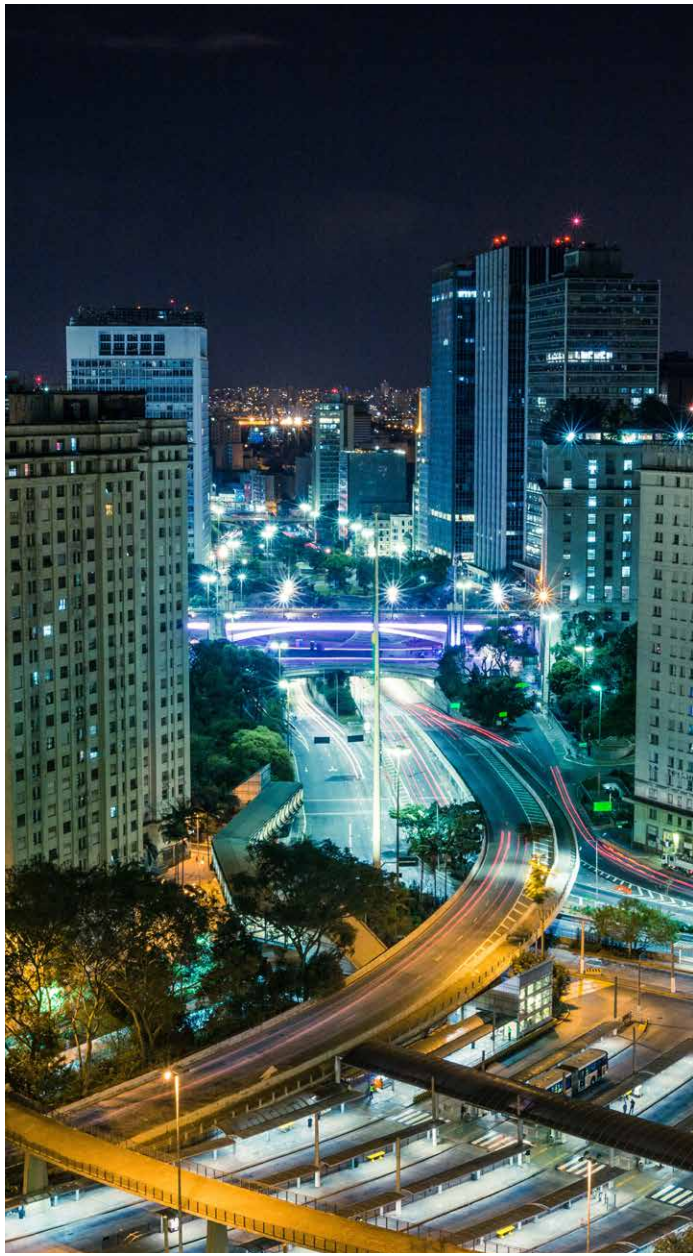
Account/Client Management

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.

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 Chargeback Services

Accertify provides fraud prevention, chargeback management, digital identity, and payment gateway solutions to customers spanning ecommerce, financial services, and other diverse industries worldwide. **Accertify's** layered risk platform, machine-learning backbone, and rich reputational community data enables clients to address risk pain-points across the entire customer journey—from account creation to authentication, activity monitoring, payment, and disputes.

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

Accertify Chargeback Services:

Accertify is a Payment Card Industry Data Security Standard (PCI DSS) Level 1 validated service provider and is ISO/IEC27001:2013 and Soc 2 compliant. The Chargeback Management solution can be used either as a standalone product or in conjunction with **Accertify's** Fraud Platform.

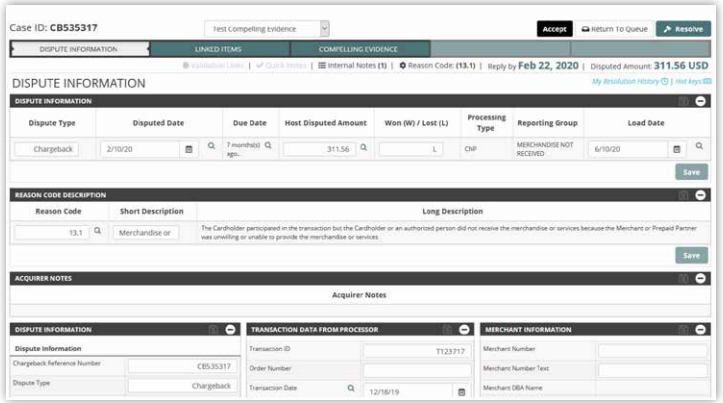


figure 1: user interface

Accertify
AN AMERICAN EXPRESS COMPANY

At a Glance:

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

Accertify Chargeback Services

Accertify's Chargeback Management solution can reduce the 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 clients can manage themselves or they can outsource the end-to-end management of chargebacks using Accertify's Managed Services offering.

The platform offers:

Automated Processor Integration: Accertify is integrated directly with most processors; therefore, most chargeback files can be automatically and systematically imported, without human intervention, 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 with the ability to create client-specific workflows based upon dollar values, chargeback reason, due date, client business needs, and other similar data points.

Workflow:
The automation of Accertify's document capture process eliminates manual processes traditionally required for uploading screenshots and printed documentation. In addition, when the workflow is coupled with data from the Fraud Platform or enhanced with compelling evidence from the client, the workflow can be designed to create fully automated responses to the processors. This no-touch model works especially well for high-volume, less complex chargebacks.

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 automated and manual intervention needs without sacrificing accuracy or efficiency.

Web-based Dashboards and Reporting: Insights provided in the reporting package allow clients to look at the big picture when assessing chargeback team operations and success criteria. The initial landing page has dashboards which display trends for recently worked items and a 12-week won\loss trend analysis. It also provides a snapshot of what chargebacks are nearing their reply-by dates. This provides a clear understanding if the client's staff are keeping up with inventory and the overall success which is being achieved.

For reporting purposes, users can select desired filters (load/resolution/sale date, agent identifier, reason code group, etc.) and can evaluate various aspects of the chargeback inventory as well as the chargeback team's productivity and success. Analyst

Accertify Chargeback Services

performance is reflected in won/loss success ratios in total dollar, case count, and percentage amounts for cases manually reviewed and complete versus total cases accepted. The platform not only provides insight into who last interacted with a chargeback but can also show an agent's average work duration for a specified period. Won/loss ratios can also be aggregated and grouped out by a reason code group, brand, and processor for trend analysis.

Lastly, the platform provides a way to export all data securely. Clients can define the data to be extracted and then run the extract immediately or schedule it for later use.

Solution Integration: Accertify's Chargeback Management solution is directly integrated with their Fraud Platform, and information is automatically populated into the Chargeback Management solution and vice versa. The Fraud and Chargeback modules form a symbiotic relationship and seamlessly leverage and benefit from one another by staying synchronized and realizing their maximum potential through the direct data share.

Accertify also partners with Ethoca, Verifi, and American Express to enable pre-chargeback capabilities related to dispute deflection, transaction clearness, 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. They do all this while providing a best-in-class customer experience to their customers.

In 2022, **Accertify's** Roadmap will focus on a few key themes, including:

- Continuing to expand acquirer/processor global footprint
- Expanding third-party shipping integrations for retailers
- Expanding and enhancing reporting capabilities and dashboards
- Developing a full end-to-end product for airlines and OTAs
- Continuing to enhance the user interface with a focus on improving client experience
- Expanding full representment automation capabilities

Sift Dispute Management

Sift is focused on Digital Trust & Safety, empowering businesses of all sizes to defend against fraud and abuse while fueling rapid growth. Some of the largest merchants in the world—including Twitter, DoorDash, and Wayfair—trust **Sift** to help deliver positive customer experiences, lower chargeback rates, and proactively prevent online fraud. With real-time machine learning, up-to-the-second signals from a global network of merchants, and a worldwide community of fraud fighters, **Sift** is committed to building long-term partnerships and helping businesses gain, and maintain, competitive advantage in their respective markets.

Sift Dispute Management

New to the Sift platform in 2021, **Sift** Dispute Management is a proven chargeback management solution that helps businesses fight friendly fraud and win more disputes—all while simplifying the customer experience. **Sift** has added chargeback management to its Digital Trust & Safety Suite to help merchants stop invalid disputes, automate evidence collection, and streamline case creation with intelligent, adaptable tools.

Solutions & Functionality

For online businesses, fighting chargebacks can be a difficult process. Dealing with numerous, unlinked sources of data can limit merchants' access to the evidence and data points they need to make decisions. It can be time-consuming and cumbersome to decide whether or not to respond to a dispute, determining what evidence to provide, and then compiling that evidence in a clear and compelling way. This can erode the ROI of the chargeback management process overall.

At a Glance:

Operational Support

Account/Client Management

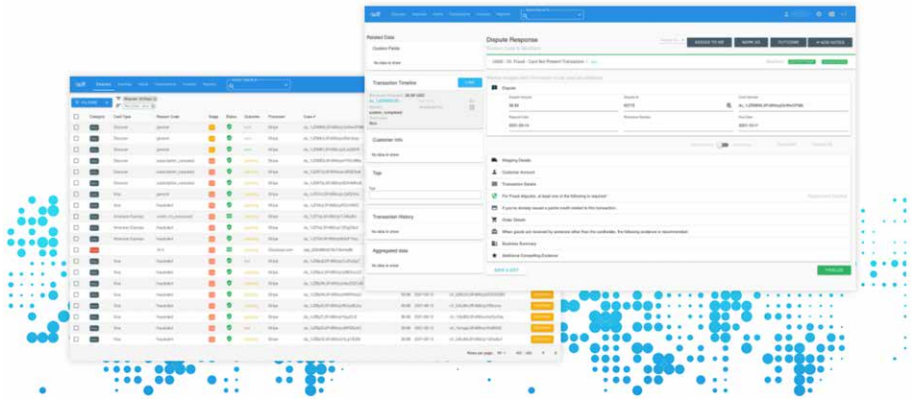
Professional Guidance/Services

Sift Dispute Management

Merchant data sources can vary, but they typically include a combination of merchant account, payment processing, gateway, sales, and order data. By consolidating the details from each source, the **Sift Dispute Management** Console allows merchants to take quick actions, such as canceling and refunding orders, and creating dispute responses. The Console provides guidance and support at each stage of the dispute lifecycle to ensure maximum recovery of lost revenue.

Most of the established providers in this market segment use a managed services outsourcing approach. Since access to dispute data is commonly gained through a gateway or processor login, this can cause problems for many merchants that are unwilling to grant access due to security concerns. To address this issue, **Sift** has 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 otherwise tedious process of creating chargeback responses, making it easy for 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 intuitively leverage 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 places. The solution is flexible enough to support a wide range of industry-specific evidence, enabling businesses to keep pace with the notoriously specific, and ever-changing requirements from each card network.



The Console provides an intelligent 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 the addition of any additional evidence application. These recommendations are provided through “tool tips,” which ensure that optimal and applicable evidence is submitted. If there are certain types of evidence that are always applied in the same way, these

Sift Dispute Management

can be automatically uploaded every time without additional user interaction.

The Console can also review the geolocation details and provide any relevant supporting documentation in the event that these details fall within a narrow radius, often a potential indication of friendly fraud. The Console can also automatically surface tracking details, add notes to indicate delivery and signature, and automatically pull data from **Sift Payment Protection** to be used as compelling evidence. In the event of true fraud, where the chargeback turns out to be valid, feedback loops can provide information back to the fraud filters to indicate why a dispute was lost.

Once complete, the dispute responses are created and submitted automatically from the Console, with the option to auto-send them to the card network, or issuer's required end-point.

Through the Console, merchants benefit from another tool: **Inquiries.** This functionality allows merchants to provide customer, order, and product details to the card brand dispute management platform—Order Insight® (Visa), and Consumer Clarity™ (Mastercard). This supplemental information is combined with the related card brand transaction data and made available to the dispute analyst at the cardholder's issuing bank. With this enhanced level of detail, the dispute analyst is equipped to make better decisions on whether to allow the cardholder to file a dispute claim—and if so, more accurately choose what type of dispute should be filed. Typically, this level of customer detail, order detail, and product detail is not made available until well into the dispute process, and can be accompanied by a message that a credit has been issued. This can also allow organizations to deflect many friendly fraud disputes, as well as chargeback fraud disputes that will be difficult to win.

Sift Dispute Management

Through integrations with Ethoca and Verifi, merchants can also receive **Alerts** in the Console. These enhanced notifications allow users to take actions to minimize losses, and prevent chargebacks from surpassing a volume that puts the merchant in danger of remediation. The integration allows analysts to be notified earlier in the process than they would otherwise. Analysts know as soon as the card companies know a dispute has been filed. These notifications enable the merchant to initiate time-sensitive actions such as stopping fulfillment, deactivating gift cards, canceling recurring billing, and suspending services. Alert coverage is continuously expanding and includes all participating issuing banks as well as fraud alerts directly from card networks.

When merchants take action based on these alerts, the proprietary system notifies the card networks directly. In the event of a refund, the chargeback can be avoided altogether, preventing negative impact to dispute rates, and potentially helping to avoid monitoring programs.

When it comes to reporting, **Sift Dispute Management** offers the most comprehensive visibility into meaningful chargeback metrics. Merchants can monitor disputes, inquiries, and alerts with a clean and intuitive dashboard view. Downloadable reports provide in-depth insights into chargeback cases, and give merchants the data they require to streamline dispute management and increase win rates.

Integrations

Sift Dispute Management can be connected through a number of existing integrations with many popular platforms, including processors, gateways, and e-commerce shopping carts. Examples include Shopify, Cybersource, Magento, Vantiv, WorldPay, Stripe, Braintree, Authorize.net, and and will soon include PayPal and Adyen. Specific merchant setup can vary based on platform. However, the list of integration partners is extensive enough to ensure seamless connections, which already exist on the provider's end, reducing the lift on merchants.

In any cases where processors, gateways, or order management systems are not already integrated, **Sift** works to identify and implement the right connections for the customer. **Sift** also provides an "Orders API" for merchants with custom-built shopping cart platforms. **Sift** can also consume webhooks and connect to existing data warehouses.

Services Offered

New customers have a dedicated Account Executive and Solutions Engineer to ensure successful integration and onboarding. Each integration is handled on a case-by-case basis and customized to use case and business model needs. Customers are also assigned a Technical Account Manager for ongoing support including continued training, additional integration assistance, and regular maintenance.

Sift Dispute Management

A team of Trust and Safety Architects, all of whom are industry experts, are available for consultation to help teams of all sizes craft a holistic, scalable Digital Trust & Safety strategy. Support engineers are also available to answer any questions about product usage and technical details. Integration, account management, regular support, and trust and safety assessments are all included. Premium support plans can be purchased based on volume and need.

In development in the next 6-12 months:

- ML-powered tooltip insights that make creating winnable responses even easier by flagging key evidence gaps and optimization opportunities.
- Increase win rates with response templates that strategically tailor to each key decision makers' (card networks, issuing banks) requirements.
- New data processing system that allows Sift to support more volume, at higher speed.
- Paypal integration that will enable businesses with high volumes of chargebacks coming through Paypal to onboard easily, and automate response creation and delivery.

ChargebackOps

ChargebackOps was founded in 2015 to combat the conventional notion that chargebacks are an inherent cost of doing business. Their services are specifically designed for midsize, ecommerce brands that prefer a customized, hands-on approach for chargebacks and order decisioning. Their method combines human intelligence with rich tool sets in order to reduce chargeback fraud, but also to help better manage and leverage the lifetime value of the end customer.

ChargebackOps' core team developed expertise with chargeback management for Visa at Cybersource. When Cybersource decommissioned the service several years ago, many clients moved to **ChargebackOps** and effectively continued being served by the same team, with many clients now having spent a decade with this highly experienced group. The analysts handle approximately 30,000 annual chargebacks and process approximately 150,000 transaction reviews annually.

Primary differentiators include:

- A hands-on, collaborative approach
- A prioritized focus toward empowering their client team's depth of fraud expertise
- A method of engagement that inherently extends the client's fraud and loss prevention team
- Operating on both sides of the ecommerce transaction: on the front-end with order screening and on the back end with chargeback management support

ChargebackOps specializes in low-risk, ecommerce markets. This is due in large part to the requirement of customized responses, which most brands demand for their customers. When considering the lifetime value of a customer for an organization, the

chargebackops
a ClearSale company

At a Glance:

Operational Support

Account/Client Management

Professional Guidance/Services

ChargebackOps

Keep authentic shoppers and build long-term customers.

last thing they want is to increase friction for a customer who has been shopping with them for 10 years.

In these cases, the client-specific-assigned chargeback analyst will decision cases with a pre-understood agreement with clients, or they may decide to discuss in real-time with each client how they would like to handle a particular chargeback. This is the nature of craft work, and the reason many customers decide to work with **ChargebackOps**.

The company's primary vertical is online ecommerce. Most of their clients also have physical storefronts for which chargebacks are processed, as well. **ChargebackOps** looks to serve, support and collaborate with companies who prioritize a long-term relationship with their customers. During the sales process, they conduct a discovery about their industry, customer handling, and approach to dealing with chargebacks.

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.
  For this reason, they do not use the one-size-fits-all approach found commonly with automated systems. They rely on human intelligence to provide customized handling for each client. The chargeback analysts work as an extension of their client's internal fraud team. The intelligence is gathered and shared with clients to identify problematic fraud trends and build new fraud rules to avoid excessive chargebacks. **ChargebackOps** handles 100% of the chargeback response process and provides clients the analytics to track and report progress.

ChargebackOps

- **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 in order to provide a conversion rate better than 90%. The expert teams help clients exceed their fraud goals at an optimized price. With order screening and chargeback management service, they operate on both sides of the ecommerce transaction. When using these services together, **ChargebackOps** offers clients with a unique fraud viewpoint, measuring and scoring both order screening quality and opportunities to further develop fraud rules. With screening analysts dedicated to each client, they can score and treat each order in a customized fashion, providing customer service experiences similar to that of a client's own employees. Rules development and management support is provided; however, **ChargebackOps** aims to empower clients to manage their own rule management process. Significant data, close collaboration, conversations, filters, and rule recommendations are provided on a regular basis. Additional ad-hoc feedback is provided by agents who review chargebacks, identifying and relaying fraud trends back to merchant clients. The feedback loop is a true differentiator. Three types of reporting are currently available, all included in the price of the service.

1. **Ad-hoc reporting available through Customer Portal:** From this portal, users can view and download pretty much any report against chargeback data. This data can be filtered by date, time periods, SKU, or BIN. The reports can be viewed within a web browser or downloaded into a CSV or Excel file, or can be emailed automatically.

2. **Twice-monthly email reports from the Customer Success team:** In these reports, an analyst reviews chargeback data to date and presents the information in a human, readable fashion. Data is easy to generate; understanding the data is an altogether different matter. The purpose of these email reports is to tell clients what the data is saying. In addition, any problematic fraud trends are brought to their attention. Solutions to these trends are recommended, including fixes to their fraud rules, customer service handling, or even product SKUs that may be generating excessive fraud.

3. **Custom analysis: ChargebackOps** analysts are frequently asked for custom reports on a wide range of data elements

including IP addresses, SKUs, BINS, etc. The team will develop any custom report for any client against any of the data they have. This could include an annual analysis, certain program or campaign-related fraud, or fraud they are seeing from freight forwarders. This is an advantage of the **ChargebackOps** solution: Custom reporting and analysis are offered at any time.

Proof-of-concept process:

Prior to, or during the initial engagement period, **ChargebackOps** will provide a 12-month look-back analysis of all chargeback-related fraud. Through this analysis, they identify fraud and non-fraud trends and recommend opportunities to reduce fraud. During this review, they will review the dispute process in place previously, the type of templates used, the data included in the template, and the timelines for submission. Customer service handling, returns process, merchant descriptor, and their service or product type, delivery, and packaging are also reviewed through this process.

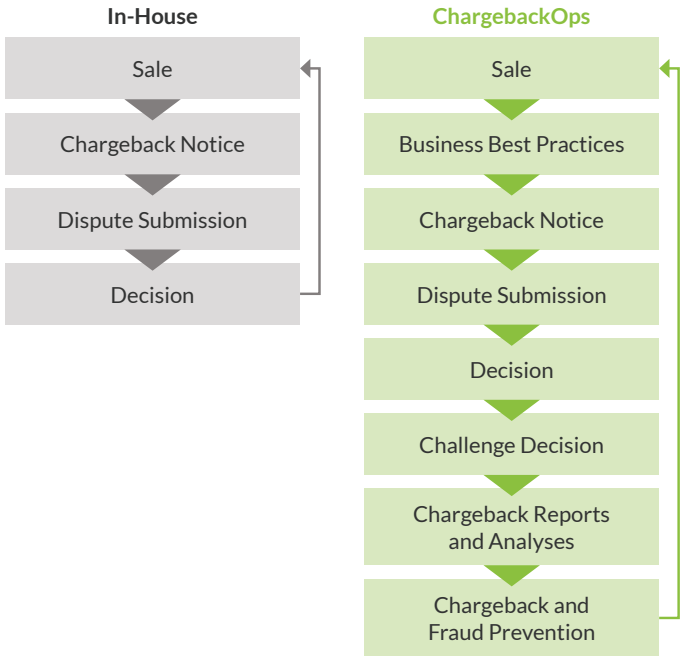
Pricing Models

Chargeback Management

While they offer a variety of pricing models, the most common approach includes fixed-monthly billing. In order to establish the fixed-monthly price, a client's past 12-months of chargebacks are reviewed and a customized quote is provided. In addition to fixed- monthly billing, a tiered structure and a hybrid recovery model/ tiered structure are available as well.

Order Screening & Review

The most common pricing model includes per-review structuring, using a Fill-A-Tier model which works by extending discount tiers once the previous tier has been met.



ChargebackOps

More aggressive pricing can be available for longer-term commitments, and for large blocks of volume, which is typically found during peak seasons, i.e., Christmas, Halloween, Valentine's Day, etc.

Integration

Because **ChargebackOps** provides a financial service and not a software solution, few integration requirements exist, with the exception of the API, which is used on a handful of clients. In each engagement, they operate more as a professional extension of a clients' internal fraud and screening teams.

ChargebackOps does use a business application that has been developed on the Zoho CRM system for internal business process workflow. Chargebacks are loaded directly from a client's processor, via CSV file or an API, and then chargeback analysts work within their Zoho CRM application. Order screening works in a similar manner; however, custom software is used to help screening analysts with efficiency and quality. A customer portal is available for each client so they can view chargeback program performance and access details they are more interested in, such as overall chargeback cases, trends, win-back rates, etc.

Their 12-month roadmap includes several new significant partnerships in 2022.

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.

Today, **Ethoca** has over 7,900 merchants and more than 5,000 issuers participating in their Alerts product globally. Since 2011, they have prevented more than 21 million chargebacks and sent more than $3.9 billion worth of alerts.

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

Solutions & Functionality

Ethoca Alerts work with merchants to prevent physical goods from being shipped, especially when they are managing the total cost of fraud. These merchants are primarily interested in stopping the delivery of goods to mitigate fraud-related losses. They also work with merchants whose primary concern is chargeback avoidance.

Ethoca works through collaboration with issuers and merchants via Alerts, essentially stopping chargebacks before they occur and allowing merchants to stop a shipment and/or issue a refund. The **Alerts** process occurs in near real-time and begins when the issuing bank notifies **Ethoca** of a fraud or customer service-related dispute.

Data provided by **Ethoca** shows that merchants are not aware of around 58 percent of the fraud that the issuers see. This allows the Alerts process to be effective for merchants.

The following diagram outlines the process:

Once they are alerted, merchants can:

- Stop the order or suspend the service
- Attempt to identify more fraud via link analysis
- Update fraud rules, strategies, or models to prevent current or future fraud
- Process a credit or refund back to the victim, which eliminates chargebacks

There are two levels of integration for a merchant: they can integrate the **Alert** data into their own platform or system via Application Program Interface (API), or they can access the **Alert** data through the **Ethoca** portal (their graphical user interface).

Ethoca white-labels their solution for one of the leading fraud prevention platform providers in the merchant space today. They also partner and integrate seamlessly with both **Accertify** and **Kount**, letting their customers obtain the potential chargeback information faster and with virtually no manual effort. This provides a more rapid response in stopping a fraudulent shipment, and/or improving their fraud rules within these platforms.

Since **Ethoca** is a confirmed fraud and customer dispute platform, and these are direct integrations, this allows the transactions from **Ethoca** to be automatically matched in their respective systems.

This makes the data more readily available for negative lists and automated features.

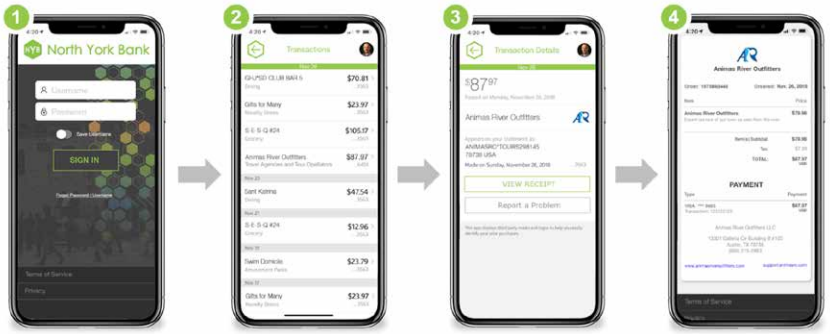
Ethoca's onboarding integration team works with customers to develop integrations. Merchants can code to the Application API and go live, which is the same for **Accertify** and **Kount**. The issuers integrate into a separate API, or may choose to provide intraday, file-based delivery to get data flowing quickly and see immediate recovery benefits.

Ethoca Eliminator

In October 2018, **Ethoca** publicly launched **Eliminator** to help reduce friendly fraud chargebacks (also known as false claims). The product was developed to prevent the chargeback at the point a customer first reports a false fraud claim to their bank. This is achieved through a merchant API integration that gives banks immediate access to a merchant's rich transaction data to prevent disputes on unrecognized transactions at the moment of first intake into the call center, or via the bank's mobile app or online statement.

For issuers, it eliminates several labor-intensive steps within their dispute management processes, including reductions in AHT (Average Handling Time) and "first call resolution," while ensuring a better experience for cardholders. This includes the cost of inbound call volume while also eliminating future purchase friction with cardholders, since cards will no longer need to be reissued when a friendly fraud claim is deflected. This will also reduce the level of false declines for card issuers' risk systems, as friendly fraud would potentially never be entered into negative files, rules, strategies, processes, or models.

There is a web-based, self-directed path that allows cardholders to click on transactions on their online banking statement for more information (essentially, the digital receipt), or via the bank's mobile app. This helps customers better recognize their own purchases and avoid having to call into their bank to report unauthorized transactions. **Eliminator** also offers a call center deployment option, allowing card issuers to enable first- or second-line agents through a simple portal, or through custom integration into the bank's dispute management systems.



Ethoca

For merchants, **Eliminator** will reduce unnecessary false declines and increase overall acceptance. Merchants benefit in two main ways from a "deflection": they immediately avoid the chargeback and also preserve the revenue that would otherwise be lost through a friendly fraud chargeback. In addition, merchants avoid the downstream representment process, significantly reducing their operational costs.

Eliminator customers are currently seeing a 35-40 percent dispute deflection rate. More than 60 merchants (including a top three digital goods platform) and 15 card issuers (including five of the top 10 U.S. banks) have now deployed **Eliminator**, with many more currently in the pipeline. **Eliminator's** functionality will continue to expand to include support for digital receipt aggregation (both Card Not Present and Card Present) and non-fraud customer disputes, as well as extended capabilities to deepen cardholders' post-transaction customer experience in the mobile app.

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.

Verifi

Verifi provides chargeback prevention in addition to having a fraud prevention platform and being a global payments gateway. At its core, **Verifi** is a Software as a Service (SAAS) based chargeback management solution. They partner with merchants ranging from start-ups up through Fortune 500 companies. They state that they stop up to 50 percent of chargebacks and they boast twice the industry average win rate on profits lost to chargebacks.

Verifi states they offer the following solutions:

- **Eliminate Chargebacks:** They stop and prevent chargebacks before they happen. They combine a **Cardholder Dispute Resolution Network** and **Order Insight**, a patent-pending platform that connects cardholders, merchants, and issuers to resolve billing confusion and disputes in real-time. This essentially gives a merchant the ability to share specific transaction-level details to the issuing bank and the customer.
- **Fight Chargebacks: Order Insight** allows clients to retain sales revenue and recover profits via chargeback representment through a service called **Premier Chargeback Revenue Recovery Service**.
- **Increase Billing:** Via **Decline Salvage**, which is logic that analyzes a merchant's transactions across broad industry benchmarks. A merchant could have the ability to resubmit declined authorizations to potentially increase authorization rates.
- **Combat Online Fraud:** A merchant has the option to utilize **Verifi's Intelligence Suite** – a "turnkey" risk-management platform.
- **Payment Processing:** This is a processor-agnostic platform integrated with over 130 major domestic and international acquirer processing networks.

They have won the Card Not Present (CNP) judges choice award for best chargeback management five years in a row.

VERIFI

At a Glance:

Verifi 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.