paladin vendor report | **fraud prevention**

2020

paladingroup

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,

Markus Bergthaler
Director of Programs, MRC

Table of Contents

The 2020 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. 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 2020 Paladin Vendor Report. We've offered previous participants the chance to update their sections and incorporated additional participating vendors.

The 2020 Paladin Vendor Report is purely informational. Paladin does not offer any opinions, reviews, or thumbs-up (or down) about the vendors contained in the report.

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 over 23 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—with many of these discussions taking place on-site. 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.

Again, this report is purely informational, and it is not designed to rate the products and services of the vendors. Its 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**
- **Identification & Data Verification**
- **Chargeback Management & Platforms**

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.

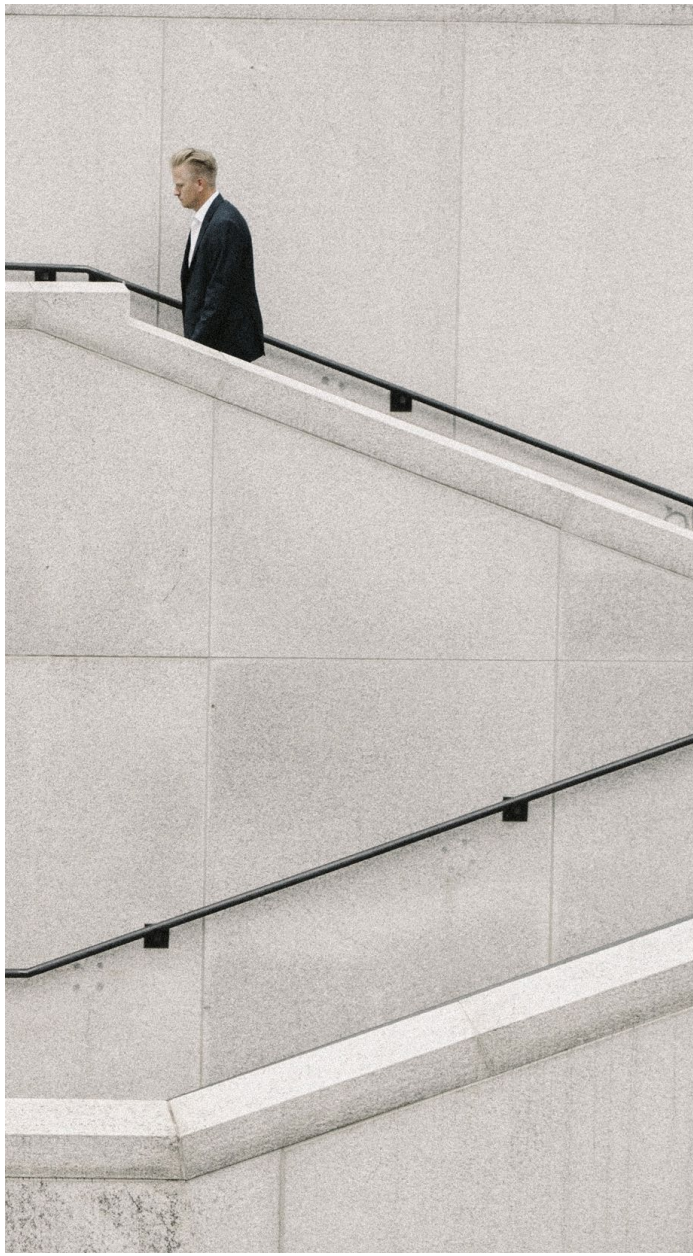
Pre-Authorization Functionality – Ability to score and/or decision a transaction prior to authorization.

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.



Featurespace

Headquartered in Cambridge, U.K., and Atlanta, U.S, **Featurespace** is a world leader in risk management for fraud prevention and Anti-Money Laundering. **Featurespace** invented Adaptive Behavioral Analytics and created 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.

Created by Cambridge University Professor Bill Fitzgerald and his then-PhD student, Dave Excell, the technology was developed at the intersection of two academic fields: data science and computer science. In his role as Head of Applied Statistics and Signal Processing, Fitzgerald built an understanding of the extraction of the "signal" (or meaning) from the "noise" in data. This notion ultimately attempts to teach machines to think like humans, separating good from bad intentions immediately and managing the behavior accordingly. In 2008, Excell adapted and commercialized this technology into **Featurespace's ARIC** platform.

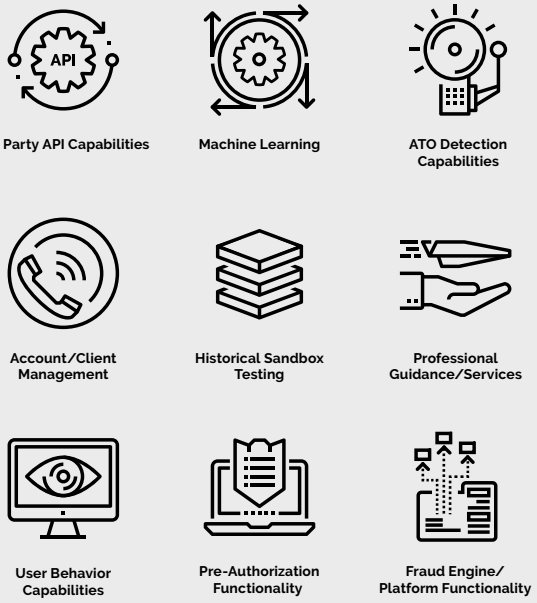
Solutions & Functionality

Featurespace's technology attempts to mimic a human-like ability to profile people over time through the **ARIC** platform, which uses Bayesian statistics to model and predict real-time individual behavior. This functionality allows computers to understand when an individual customer's behavior is out of character and automatically evaluate 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 50.4 billion transactions worldwide.

FEATURE SPACE

OUTSMART RISK

At a Glance:



Featurespace

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. And if clients manage their own data science models, the technology allows clients to import these models alongside the **ARIC** platform's own.

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.

ARIC Risk Hub: A typical transaction follows six steps in real time while observing multiple data points over time.

1. **Data streams are input:** multiple internal and external sources of data are processed (determined with the client).
2. **Signal extraction:** behavioral signals are extracted from the data at both individual and group levels.
3. **Anomaly detection:** behavioral anomalies are identified in real time.
4. **Individual predictions are made:** based on the likelihood of committing acts, such as fraud or illegitimate product purchases.
5. **Action is taken:** the **ARIC** Risk Hub user interface is fed with real-time information so a fraud analyst can take appropriate action. The transaction is accepted, denied, or step-up authentication is requested automatically.
6. **Self-learning system feeds results back into ARIC:** updating profiles in real time.

Merchants of all sizes can take advantage of the benefits of the solution. Large, enterprise-scale merchants can integrate directly, managing the functionality with internal resources, while smaller merchants can potentially take advantage through an acquirer who is integrated upstream, helping to manage inherent transactional risk.

Featurespace

Featurespace has developed a number of industry partnerships ranging from well-known payment service providers to fraud data providers:

- Along with committing an investment, Worldpay has formed a commercial partnership with **Featurespace** to help accelerate the development of fraud prevention services for Worldpay's own merchant customers. As part of the agreement, Worldpay will license **Featurespace's** behavioral analytics technology for a number of use cases, including risk management and fraud prevention for merchants. This will allow existing Worldpay merchant clients to take advantage of the **Featurespace** technology without requiring full integration.
- **Featurespace** partnered with TSYS to deliver the TSYS **Foresight Score℠** with **Featurespace**. Clients have access to a layered approach to stop fraud in real time. Most recently, TSYS also chose to build the TSYS Authentication Platform based on the results achieved using the **ARIC** platform as the basis for their **Foresight Score℠**.
- **Featurespace** has also partnered with **Ethoca** (also featured in this guide), feeding **Ethoca** alerts in the **Featurespace ARIC** system. These alerts expedite the receipt of chargeback data, reducing the delays in receiving this data and in receiving subsequent model updates.

The partnerships with Payment Service Providers can help entities better manage acceptance, as it creates an environment with an increased level of integration. For example, combining known historically high-risk criteria with the observance of low-risk behavior at all points of contact can improve performance and reduce false positives.

Featurespace

Services Offered

During integration, **Featurespace** can work with the format of the data provided. They want to make sure business users can work within a format they're familiar with. This applies to outputs as well, which can be defined to match the client's existing format.

Requirements include transaction history and confirmed fraud (the amount of historical data needed is determined with the client), which allows **ARIC** to profile and track good behavior (bad behavior is identified by what's left). This focus on good behavior helps clients to drive down false positives while identifying suspicious activity, which could also indicate new and unknown fraud types.

Client touchpoints vary based on integration type. Clients can integrate through a partner (such as TSYS, Worldpay, or others) as the relationship between the partner and **Featurespace** already exists. Full environment integration via cloud or on-site can take as little as four weeks, depending on client requirements, prioritization, and resources available.

Throughout its services, **Featurespace** focuses on three pillars of customer interaction.

- **Customers and advocates:** Clients experience substantial face-to-face interaction. Service and sales agents get to know clients personally and understand their product needs.
- **Subject matter expert team:** This includes a deep understanding of what's going on in the industry and what clients need. This also feeds into the development of the **ARIC** platform.
- **Global marketing and events:** Featurespace hosts and attends several events throughout the year. This includes both leadership content and client participation.
- **Featurespace's Customer Success team:** The team builds strong relationships with their customers, gaining deep understanding of their business and providing relevant updates on best practices and the latest product features. The team also serves as an escalation point of contact and commercial advisor for additional requirements and renewals.

Service agents are involved beginning with the initial sales interaction. The agents establish a relationship and identify business drivers and key objectives (such as reducing fraud or increasing acceptance). During the onboarding phase, it's important to understand data sources and train models. Once live, the focus shifts to continued service, with dedicated account managers and with 24/7 support available.

Featurespace

The goal is to create uniformity throughout the process, from design to delivery, with the understanding that specific skillsets are required at each stage.

Three pricing models exist:

- **Integration inside client environment** (on-premise) with an annual license fee. Transaction fees still occur, but these are often included in the license.
- **Perpetual license** comes at an upfront price with support and maintenance fees. These are tied to a fixed-term support contract.
- **Fixed-term agreement** with fixed fee is managed in the cloud and fully outsourced in a SaaS model, with a set number of transactions included and transaction fees for overages.

NuData

NuData is a Mastercard-owned company headquartered in Vancouver, British Columbia that specializes in device analytics, behavioral analytics, and passive biometrics. Since its inception in 2008, it has maintained a heavy focus on research and development while looking for better and more sophisticated ways to distinguish automation from human and delineate good users from risky ones.

Their flagship platform, the **NuDetect** suite (launched in 2013) marries enhanced device intelligence, behavior, and passively collected biometric data to analyze and protect high-risk touchpoints throughout merchant and financial institution environments. The platform processes billions of events yearly.

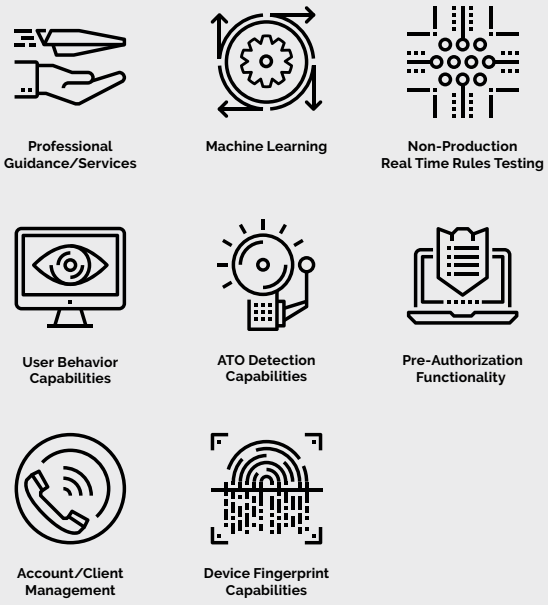
In addition, **NuData** offers a risk-based 3D Secure (3DS) solution harnessing the power of the **NuData** technology, where businesses can benefit from the new protocol combined with behavioral biometrics.

The company's acquisition by Mastercard provides additional stability and brand recognition as well as increased data volume and visibility into the Mastercard ecosystem. Recent developments include application of **NuData** technology into Mastercard's Masterpass secure remote checkout (SRC) as well as integration into Mastercard's MPGS gateway and fraud solutions.

NuData Security

mastercard

At a Glance:



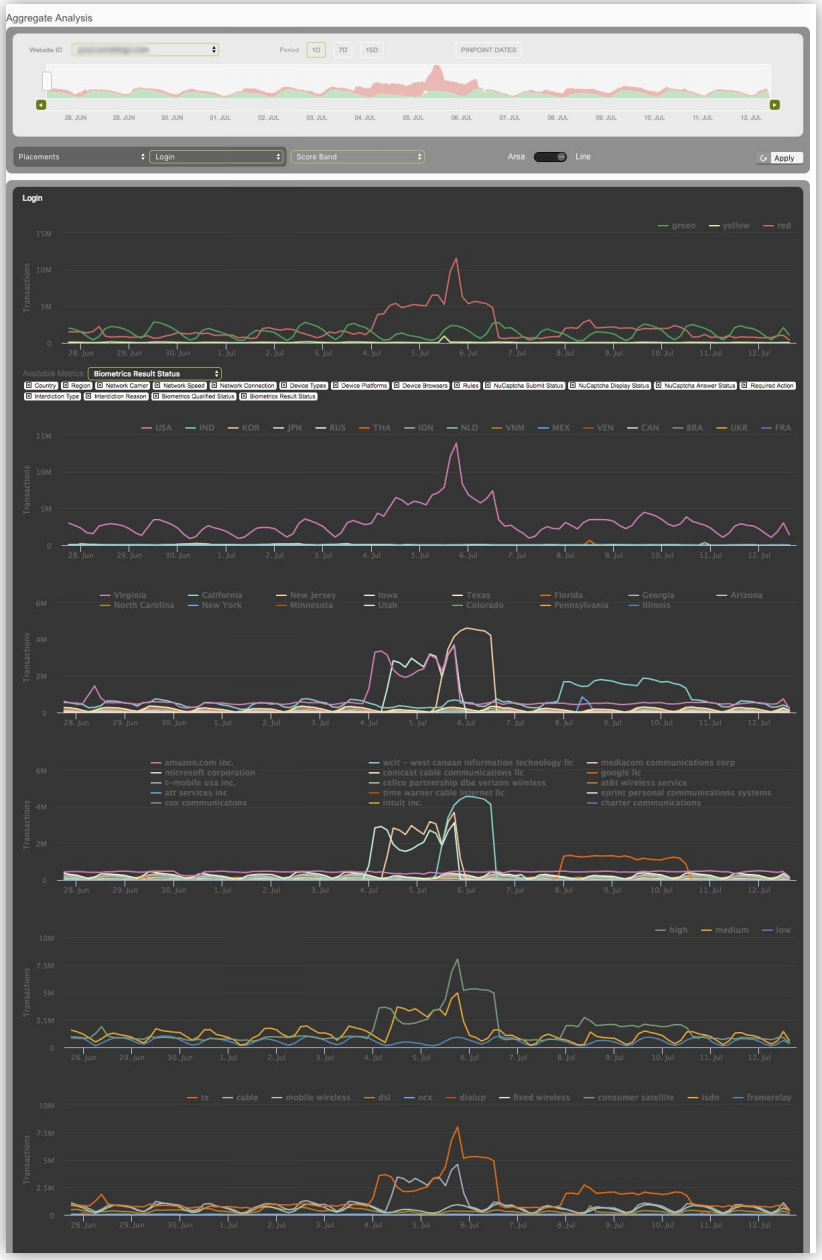
Solutions & Functionality

NuData uses a multilayered approach to understand a user's digital interactions, analyzing the user across device, location, connection, behavioral analytics, passive biometrics, and the **NuData** Behavioral Trust Consortium.

NuData's technology, and its **NuDetect** platform, are offered as a group of solutions targeted to specific industry pain-points and use cases. As such, **NuData** offers specific products that protect from automated attack risk (**NuDetect** for Automation), account takeover risk (**NuDetect** for ATO), account creation fraud (**NuDetect** for Online Account Origination) good user verification (**NuDetect** for Good User Validation), device intelligence (Mastercard Trusted Device), and EMV 3DS solution (Smart Interface). These products can be sold together or separately, and can be useful to large and medium-sized businesses. **NuData** continues to identify potential use cases for custom client integration that support new and unique business models.

NuData solutions cover the following use cases:

Account Takeover Risk: With the amount of personal data readily available on the dark web, ATO attempts are on the rise. **NuDetect** for ATO helps protect against this behavior, **NuData** uses behavior as well as a host of additional data points to validate legitimate logins. The account is then analyzed in real time across the entire session to ensure there are no sudden changes in behavior.



This can help clients by:

- Stopping scripted attacks at login
- Increase confidence in customer interaction
- Reduce friction for trusted customers

Automation Risk: To manage scripted attacks, **NuDetect** for Automation tracks deviations in the traffic behavior to identify automated and nonhuman risk at any placement. Changes in expected behavior like browser type, surfing speed, and time-on-page are powerful risk and fraud indicators.

This can help clients by:

- Stopping scripted attacks at login
- Increasing focus on good customers
- Boosting trust in the environment

Account Creation Risk: The number of data elements available to malicious users represents an endless resource for new account fraud. When users apply bits of legitimate identity, verifying these accounts can be difficult. Through the four-layer approach, **NuDetect** for OAO evaluates whether the user is behaving like a legitimate user, or like a fraudulent user or a bot. These high-risk accounts are flagged, so the appropriate steps can be taken.

This can help clients by:

- Preventing future fraud
- Avoiding fraudulent transactions
- Reducing operational costs

Frictionless user experience: By utilizing passive biometrics as well as billions of behavioral profiles, **NuDetect** for Good User Verification can help clients recognize legitimate users from login to logout and at every interaction in between. This can be used to provide users with an enhanced experience.

This can help clients by:

- Preventing false declines
- Build a relationship with good clients
- Remove unnecessary friction

Device Recognition: A subset of the **NuDetect** technology, focuses on recognizing returning devices to prevent fraud. This can be implemented as a stand-alone solution, an option especially interesting for small and medium businesses.

Trusted Device, an enhanced device-recognition tool, allows users to re-bind devices that have been wiped (including removal of cookies, modification of operating system, etc.). Because of the device changes, device intelligence tools can track a device up for an average of 22 days. Trusted Device can track a device for 140

days. "Mastercard Trusted Device" will soon be integrated with all web-based products Mastercard is rolling out. And, post upgrade, the benefits are immediate.

End-to-end security: High-risk interactions can take place at numerous locations within a given environment. For example, for a user to fail 30 times at login and then go on to make a purchase is very suspicious, but this can only be detected if the different placement security is connected. **NuDetect** for Continuous Verification continuously monitors user behavior across the entire session and allows to block these users in real time.

This can help clients by:

- Prevent fraud at any step
- Detect account hijacking
- Remove unnecessary friction on trusted users

EMV 3DS transactions: Smart Interface is the Mastercard and **NuData** offering that provides the ability to authenticate a transaction using the EMV 3DS standard (along with 3-D Secure fallback to the 1.0 standard). This solution includes **NuData's** behavioral security at checkout as well as rules and policies system. Smart Interface allows merchants to evaluate the risk of a purchase before 3DS processes it. Merchants can also build rules based on the risk level to process a transaction through 3DS or to process it outside of the 3DS flow (data only flow).

This brand-agnostic solution is available through a single Software Development Kit (SDK) whereby a client can implement the 3DS service as well **NuDetect** at checkout. The service is especially popular in the EU where applicable law and regulation have yielded adoption of the Smart Interface solution by the merchant community.

The technology that supports the NuData solutions:
NuData's strength lies in its intelligence, built on four integrated layers of technology to build an accurate picture of each user's risk profile. The behavioral data across account, device, and network is anonymized. **NuData** continually analyzes this data to identify anomalies, spoofing, or unexpected user behavior.

This intelligence is generated and shared with **NuData** clients in real time, allowing them to accomplish two key goals. First, they identify high-risk users and activities, before a submission–allowing merchants to deploy risk-mitigating controls only in high-risk situations. Their second goal is to provide a better experience to legitimate users.

NuData leverages the following four layers to build a reliable profile of each user:

1. Passive biometric verification: NuData's passive biometric analysis screens how the user interacts with the device. This includes the collection of hundreds of features like typing speed, keystroke

deviations, key up/down analysis, accelerometer data, and the way the device is spatially oriented. Passive biometrics allow **NuData** to achieve three key objectives.

- First, determine if the user interacting is human or nonhuman based on how the user is physically interacting with the device
- Second, if the user is human, **NuData** identifies if it is an anomalous human.
- Third, **NuData** then identifies whether or not the human is the expected human, or if it is a malicious individual with stolen authentication credentials.

2. **Behavioral analysis: NuData** attempts to understand how the data analyzed relates back to historical data linked to that user. For example, if a user has always interacted on a Mac using the Safari browser, it would be expected for that user to use a Mac with the Safari browser during future interactions.
At the population level, **NuData** looks to understand how the ratios of data are passing through the overall environment. For example, if the environment traditionally sees its overall user-base interacting via Chrome 20% of the time and Internet Explorer 35% of the time, it would be expected that these ratios would remain relatively stable. If **NuData** starts to identify deviations in the expected data ratios, it can recognize these anomalous subpopulations to understand better if a risk is present.

NuData analyzes hundreds of data points in real time across both the individual user and full population to identify anomalous or risky behavioral interactions.

3. **Device, location, and connection intelligence: NuData** analyzes the user's device, connection, and location during each behavioral profiling event. This data is used to understand how the user is connecting to the environment and with what device type. This allows **NuData** to understand if the user is coming from a device/connection that is expected, or if the device/connection is attempting to spoof or obfuscate its true information.

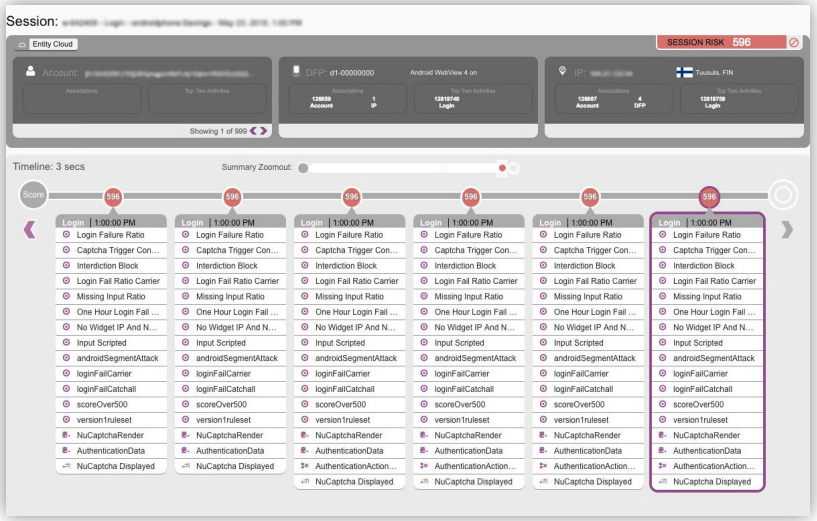
4. **Behavioral Trust Consortium: NuData** holds the world's largest behavioral network, with over 650 billion behavioral events analyzed only in 2019. This consortium brings together the billions of data points collected across **NuData** clients to create a positive-pattern and negative-pattern consortium. During each monitoring event, **NuData** collects and anonymizes key data points, which are promoted into the **NuData** Trust Consortium. Positive and negative quintile rankings are assigned to these data points based on the level of risk or validity identified. This intelligence provides further insight during a behavioral profiling event.

NuData

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. 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. Using this connection, **NuData** provides the same level of security for users and stops all forms of basic and sophisticated attacks.

How does NuData work?

At each behavioral profiling point of interaction, **NuData** generates a score array consisting of a set of behavioral scoring elements that are returned to the client environment in real time. The score is generated based on the analysis of the user's device, connection, behavior, and passive biometric data collected during each behavioral event, and any relevant data from the trust consortium. The following section provides an overview of the types of intelligence provided by **NuData**.



Components of that decision can include the following:

- **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, phone, 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.

NuData

- **Score: NuData** generates a numeric score that provides a risk value for the event profiled.
- **Score band: NuData** passes back a Green/Yellow/Red score band identifier based on the total score generated for the event.
  - **Device ID: NuData** creates a token-based Device ID that provides an exact device identifier to determine when a previously profiled device is returning to the client's environment.
  - **Device fingerprint: NuData** provides a configuration-based device fingerprint that offers a lower-resolution device identifier that can be used to group similar device configuration types.
- **Behavioral intelligence signals: NuData** generates behavioral intelligence signals at each event profiling. Behavioral intelligence signals provide additional context into the risk or lack of risk identified during each profiling event.
- **Real-time evaluation:** Real-time rules and policy explanations, using "NScript" (an easy-to-use rule language), gives users insight into the specific rule combinations triggered. NScript can also let users create and manage their own rules. These rules can stand alone or be placed in "rule families," which can be focused on specific attack types, automation, account takeover, etc.
- **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 captcha. Along with providing the full enforcement solution, **NuData** can intelligently alert when in-house client interdiction enforcement policies should be triggered.
- **Client dashboard:** The client dashboard provides the client with full real-time visualization of behavioral intelligence data collected on the web, mobile, native app, or API environments. The portal displays the environment at multiple levels spanning from the full aggregate view, individual user profiles, session interaction analysis, and aggregate behavioral analysis visualization. The interface can drill down and provide extensive details for each activity, pivoting on signals (or rules) and placement (touchpoints mentioned above).

NuData offers an uptime service level agreement (SLA) of 99.7 percent, and typically sees uptime above 99.9 percent. **NuData** offers an SLA of 300ms for processing time, and actual performance is considerably faster.

Customer support for clients

When working with **NuData**, clients receive a customized service approach. Unlike some solution providers who offer general service packages, they attempt to truly understand the goals and needs of the client and provide service levels aimed at meeting those needs. With the increased functionality centered around EMV 3DS **NuData** has also expanded its international service footprint in the E.U., Asia Pacific, and Latin America.

Customer service prioritization follows a three-tier process:

- 24/7 emergency support: A 15-minute response SLA, including outages, major performance issues, etc.
- Non-production impacting: A 24-hour response SLA
- Customer success manager: Offered as needed, such as for a long-term strategy
- 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.

A typical project track would progress through a three-phase process:

1. **Project scope and kickoff:** Customer success is engaged throughout this process, with emphasis on success and implementation criteria. It includes one to two days of scoping meetings to identify the use cases, placement mapping, identifying success criteria, technical walk-through, and review of the integration documentation.
2. **Integration and development:** The full integration (including scoping, documentation, and implementation) can take as little as two weeks, but the average timeframe is four weeks depending on the number of touchpoints and teams involved.
3. **Post-coding analysis and optimization:** This stage includes implementing models in silent monitoring mode to allow analysis and model behavior. Next is a collaborative tuning phase, with a 30-day learning period typically required for high-probability performance.

BehavioSec

BehavioSec is a behavioral biometrics platform vendor. They state that they use continuous authentication and behavioral biometrics via machine learning to protect merchant customer accounts.

BehavioSec analyzes activity via algorithms, from login to logout, and looks at keystroke dynamics, touch, and mouse motion. It then compares it to previous interactions from the same user. It then creates a score that is fed into a merchant's fraud engine and creates a step-up for authentication. There is also a dashboard to see their score breakdown and identify behaviors or anomalies.

They also have bot detection capabilities as well as the ability to detect things like password managers, copy-and-paste actions, and tabbing between fields. Their system allows merchants to define their risk appetite via whitelisting good users and force-retrain, and merchants can see a detailed audit trail of user sessions.

BehavioSec offers continuous real-time authentication to give a merchant protection across a session by breaking down the characteristics of fraud or breach type. Their flags include spotting a change in device or IP address during a session, or bot activity.

BehavioSec

At a Glance:

Machine Learning

User Behavior Capabilities

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.

Cyberfend

Cyberfend specializes in bot and automation detection. The solution detects attack scripts, deployed in any language through any system on any device, under any platform. It focuses on verticals that have become targets of stolen credit card use. These include ecommerce, online banking, online sharing, social networks, travel websites, online ticketing, educational services, healthcare, insurance, and gaming.

These attacks typically originate from individuals attempting to monetize stolen credentials across a wide range of popular web and mobile services. These fraudsters know that people commonly reuse their credentials across the web. **Cyberfend** has built the real-time detection capability to address login and payment deficiencies that allow these kinds of schemes to succeed.

CYBERFEND

At a Glance:

User Behavior Capabilities

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

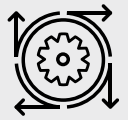
DataVisor

DataVisor's outlook is that fraud detection should be automated. Because of this, their approach to transactional risk mitigation is through unsupervised machine-learning technology. Unlike solution providers who rely on a machine-learning approach, they are using clustering technology to associate users and events rather than labels to distinguish between "good" and "bad" behavior. This non-reliance on labels can help combat the "training" period required by many machine-learning-based platforms, and it also helps eliminate as many unknown unknowns as possible.

Because of the automation associated with the platform, they are able to create and modify rules on a daily basis. This helps mitigate attacks before they get big. Along with tracking risk associated with the transaction itself, they have the ability to track other types of events such as login, browsing session, account modification, etc. Device ID functionality is also available. They boast that the complete platform is very precise, delivering a low rate of false positives.

DATAVISOR

At a Glance:



Machine Learning

User Behavior Capabilities

Pre-Authorization Functionality

DataVisor 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.

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.

CardinalCommerce

For over two decades Cardinal has been bringing merchants, issuers, and shoppers together. In February 2017, **Cardinal** became a Visa solution. They put authentication first and believe digital commerce should be as safe, trusted, and engaging as possible.

Navigating the ever-changing payments landscape can be complex, amid local regulations, different network mandates, and **EMV® 3-D Secure** updates. Which is why their dedicated success teams work closely with clients from integration through ongoing optimization to make the process as frictionless as possible for both clients and their customers.

Their primary focus is on creating an engaging experience for both clients and their customers. They work continuously to help optimize authentication strategy to increase approvals while decreasing fraud – all to improve the customer journey.

More key facts about **Cardinal**

- Offers merchant and issuer authentication solutions.
- Certified by EMVCo for four **EMV® 3DS** components – ACS, 3DS Server, iOS SDK and Android SDK (Source: https://www.emvco.com/approved-registered/approved-products/) .
- Focused on authentication, supported by a team of more than 200 people.
- Can help merchants and issuers prepare for the next round of Visa activation dates for EMV 3DS – April 2020 in AP and CEMEA, August 2020 in NA.

At a Glance:

3rd Party API Capabilities

Pre-Authorization Functionality

Account/Client Management

CardinalCommerce

Intelligent Security, using the Visa family of risk solutions, can help digital commerce business increase authorization rates and reduce false declines and fraud. Visa's intelligent security is a multilayered, data-driven framework that delivers streamlined consumer experience.

- **CardinalCommerce** – for 3-D Secure/authentication
- CyberSource – for fraud management
- Verifi – for chargeback dispute resolution
- And other Visa solutions

With this suite of solutions, Visa can help merchants, acquirers, and issuers deliver a seamless, secure experience for the consumer.

Solutions & Functionality

What Cardinal solves for

Cardinal's focus is on authentication. They are highly focused on all aspects of authentication so that merchants and issuers have the best resources, backed with more than two decades of experience, and can focus on technology, security, and people.

Cardinal uses data with a goal of driving higher approval rates for issuers and merchants with a number of payment decisioning solutions, including 3-D Secure.

By using **EMV 3-D Secure**, merchants and issuers can access even more data in the authentication process, so that they can be more efficient and effective when assessing transactions for potential risk and fraud. This is because of the connection on both sides of transactions through **Cardinal**, with the 3DS Server and the ACS. The enhanced **EMV 3DS** data can be shared directly with the issuer, not only for authentication, but authorization as well. Through **Cardinal** Consumer Authentication (CCA), merchants can communicate with the issuing bank and share data about the consumer, their device, and the transaction. It allows the issuer to make a more informed, more confident risk decision. **Cardinal's** solutions support all of the major card networks. They do it while adhering to government mandates and other regulations, which can introduce complexity into the whole payments system.

How it works

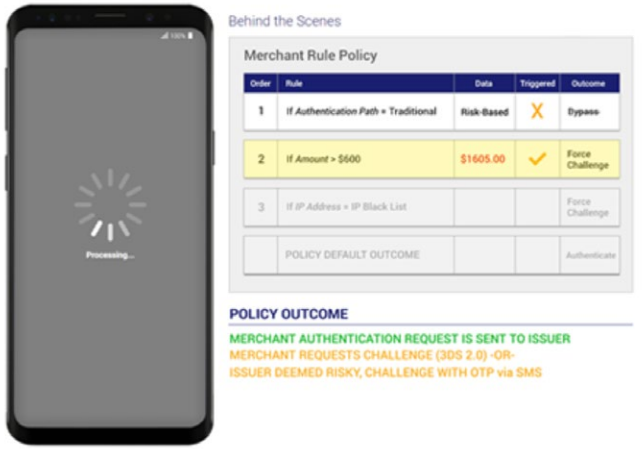
The image above shows what happens after the consumer submits their order. More than 100 **EMV 3DS** data points are shared with the issuer, to help them make their risk decision.

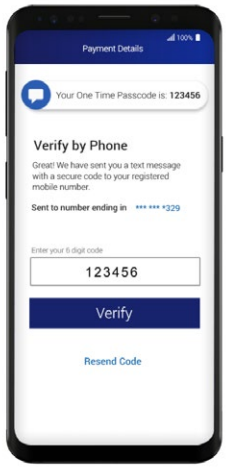
There are instances where a challenge is necessary when using **Cardinal Consumer Authentication**, but most transactions can be authenticated behind the scenes, with little-to-no consumer friction, due to the robust data shared with the issuer. (Note that in the European Economic Area – and other regions where there are government mandates in place – digital transactions that are subject to Strong Customer Authentication or another two-factor authentication requirement may experience some friction during authentication). As for the "risky" transactions that need to be challenged (or transactions challenged because of SCA), the issuer can ask for more information from the consumer (vs declining the transaction at that point) and challenge through, for example, a one-time passcode (OTP) (sent to the consumer's email or mobile device) or a biometric.

This functionality, and the ease with which the consumer can complete the step-up, allows the merchant and the issuer to complete transactions that would have otherwise been deemed fraudulent and declined.

In this scenario the merchant is able to sell their product, the issuer is able to collect funds, and most importantly, the consumer is able to buy what they want, from the merchant they choose, using their preferred card.

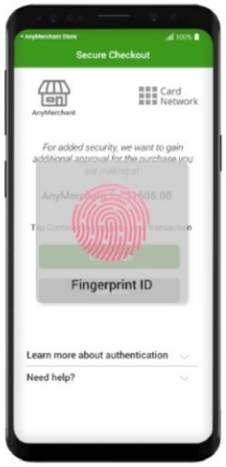
The images below show what happens during the challenge. In the first graphic, the merchant's risk rules trigger a challenge (the issuer's risk rules can also trigger a challenge). The merchant communicates that with the issuer, and the issuer sends the consumer a one-time passcode on their mobile device or can challenge using a biometric like a fingerprint. Both are illustrated here.





Consumer receives the OTP, enters it, then clicks the "Verify" button to complete transaction.

CardinalCommerce

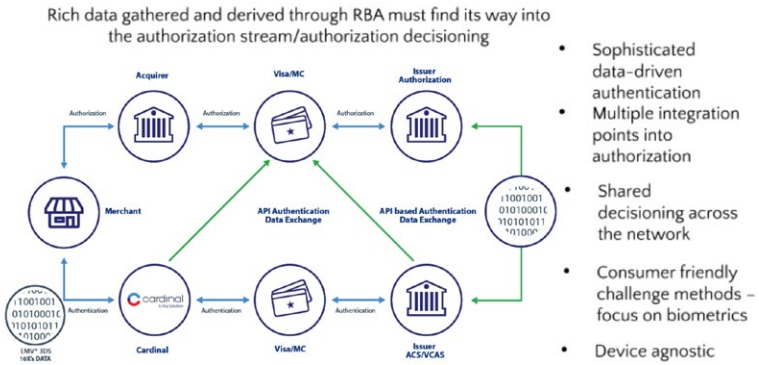


Challenge
Biometric Fingerprint

The consumer clicks "Continue" to begin the biometric Fingerprint ID authentication feature.

How Cardinal does what they do

When **Cardinal** authenticates transactions, the flow is relatively seamless. The diagram below outlines the steps that are taken as a consumer checks out with an online merchant. Prior to authorization, authentication takes place, and in most cases, the authentication process happens behind the scenes without friction during checkout.



Benefits of using Cardinal Consumer Authentication:

Fraud Decreases: Overall, CCA helps remove fraud from the entire digital payments ecosystem through the collaboration of merchants, issuers, and **Cardinal**. Using the enhanced data (on the transaction, the device, and the consumer), merchants can reduce the frequency with which they manually review their riskiest transactions, opening more time for other business functions.

More Transactions Can Be Authorized: Since the issuing bank is doing the risk assessment during authentication, they can approve more transactions during the subsequent authorization process. This can help increase sales and reduce false declines.

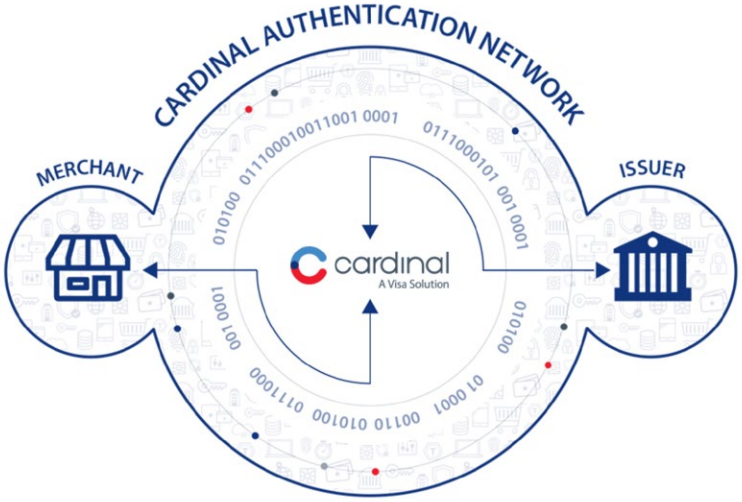
Better Consumer Experience: For issuing banks, this solution can reduce friction for their cardholders during checkout. Since authentication happens behind the scenes, consumers are not interrupted during checkout.

The Cardinal Authentication Network: authentication solutions for merchants and issuers for better results

The **Cardinal** Authentication Network joins merchants and issuers so they can share what each knows about their mutual consumers, to achieve the goals of more authorizations, less fraud and fewer false declines.

Cardinal is unique in that they work with tens of thousands of merchants (with **Cardinal** Consumer Authentication) and thousands

of issuers (with Visa Consumer Authentication Service), providing authentication solutions throughout the transaction. **Cardinal's** work with merchants focuses on reducing fraud, chargebacks, and false declines to help increase authorizations, using enhanced data for authentication and delivering a better consumer experience.



With the ability to route transactions through the appropriate 3DS version, 3DS 1.0 or **EMV 3-D Secure** (formerly known as **3-D Secure** 2.0), Cardinal enables merchants to benefit from authentication. **Cardinal** Consumer Authentication, their merchant solution, gives merchants control and allows them to strategically decide which transactions to authenticate silently and which to step-up, via dynamic rules.

With CCA, merchants share additional data about the consumer, the transaction, and the device with issuers, who can then make more confident risk decisions without impacting the consumer's checkout experience (except in regulated regions).

Together, **Cardinal** Consumer Authentication (the merchant solution) and Visa Consumer Authentication Service (the issuer solution) focus on both sides of the transaction, and commit to working with both merchants and issuers to bridge the information gap during authentication. **Cardinal's** unique advantage results in reduced fraud, false declines, and manual reviews—and it helps increase sales.

About Cardinal's Support and Customer Success Teams

Cardinal takes pride in their secret weapon, the Support and Customer Success teams. Many of their team members have been with **Cardinal** since the early days and are experienced in helping merchants and issuers manage their authentication strategies.

Cardinal's Global Client Services Group supports their clients in a variety of ways.

Solution Engineering and Implementation teams are dedicated technology Subject Matter Experts (SMEs) who are focused on understanding the needs of **Cardinal's** merchants and issuers. They use **Cardinal's** technology to design and deploy a custom-tailored authentication strategy for customers.

CardinalCommerce

Customer Success teams have one primary goal: to guide customers navigating the complexities of the payment authentication ecosystem. They also provide ongoing support and client management for **Cardinal** Consumer Authentication and Visa Consumer Authentication Service, **Cardinal's** merchant and issuer solutions. They accomplish this by collaborating with customers to create a custom authentication strategy to maximize the ROI when performing 3-D Secure.

- **Cardinal's Customer Success managers** are well versed in the ever-changing authentication ecosystem. They work with merchants, payments industry partners, and financial institutions. Together, they develop a roadmap to implement and deploy **EMV® 3-D Secure** for the 2nd Payment Service Directive (PSD2) requirement for Strong Customer Authentication (SCA) in Europe. They help merchants and issuers comply with other government mandates, as well. This team provides analytical insight to their customers, using data and industry trends to help them stay ahead of the curve.
- **Support and Technical Account managers** also offer full technical support to their customers and partners, 24/7, every day of the year, through a variety of channels. These include a web-based ticketing system, phone, email, status page, and a client management team in their Ohio headquarters.

In the next 6-12 months:

- Payment decisioning solutions like Data Only
- Additional SDK updates and solutions
- VCAS feature enhancements for issuer ACS
- PSD2 Smart Detection and Exemption Management capabilities – services to support PSD2 SCA in Europe as preparation continues in advance of enforcement dates
- Upgraded Merchant Portal

RSA

RSA helps merchants detect, review, and respond based on internal business decisions. This is achieved by offering merchants visibility into how users are behaving and interacting within their environments. In addition, they can provide industry insight into what's happening outside a merchant's environment to help them prepare for potential future threats. They believe that a solution must have the complexity to distinguish between legitimate users and criminals demonstrating similar activity.

They also believe that fraud solutions must provide a specific list of benefits:

- **A balance of security and convenience** to maximize fraud detection while minimizing customer friction and false positives
- **Rapid, actionable insights** that deliver results quickly and in a consumable way
- **Visibility into the entire ecommerce environment** should go beyond checkout
- **A focus on business-specific priorities** should support a strategy based on merchant-specific levels of acceptable risk
- **A focus on business impact** will ensure the above levels of risk and acceptance are maximized

As soon as users hit the merchant's environment, **RSA® Web Threat Detection** begins to monitor their behavior. This continues throughout the active web session, allowing the solution to expose all online activity in real time, capturing as many available variables as possible. This functionality allows **RSA** to provide segmented web traffic, analyzing various aspects of the web session and applying them uniquely across verticals.

RSA 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.

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.

iovation, a TransUnion Company founded in 2004, is a Portland-based device-based fraud prevention and authentication solution provider. Their original aim still rings true: "To make the internet a safer place to do business."

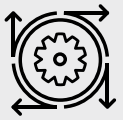
iovation's global device network offers a consortium informed by experience with over 6.5 billion devices seen and 76 million reports of fraud and abuse, and **iovation** has over 200 employees globally. They use proprietary technology to capture unique identification for devices that interact with a merchant's site. Real-time responses average 100 milliseconds, and their system uptime service-level agreements (SLAs) are 99.9 percent. Since the **Transunion** acquisition of **iovation**, the two have combined forces to offer an end-to-end solution (discussed on pages ## - ###). However, their device-based reputation, fraud prevention, and authentication solutions are offered as stand-alone products, which we will discuss below.

Solutions & Functionality

FraudForce device-based reputation offers real-time fraud prevention using device intelligence. **iovation's** proprietary fingerprint technology offers merchants the ability to recognize devices that interact with them and assess for risk factors indicative of fraud. As part of the **iovation** consortium, a merchant can leverage information based on **iovation's** experience with over 6.5 billion devices and over 76 million known fraudulent events. **iovation's** database contains the industry's best retention history—data on fraudulent devices and granular fraud report records are kept for five years after inactivity and indefinitely for active devices.

iovation®
A TransUnion® Company

At a Glance:


Machine Learning


Account/Client Management


Device Fingerprint Capabilities

This device-based solution can help prevent online fraud, including application fraud, credit card fraud, identity theft, and account takeover. The device fingerprint technology allows a merchant to establish different risk thresholds for devices with suspicious behavior based on inconsistent or missing data elements. Some elements include anonymizing proxies (such as Tor), geolocation mismatches, high-risk locations, Internet Protocol (IP) addresses and Internet Service Providers (ISPs), and jailbroken or rooted mobile devices. **iovation's** user interface lets merchants create rules for weighting and subsequent scoring. The UI also enables reporting, tagging fraudulent devices and accounts, and managing teams.

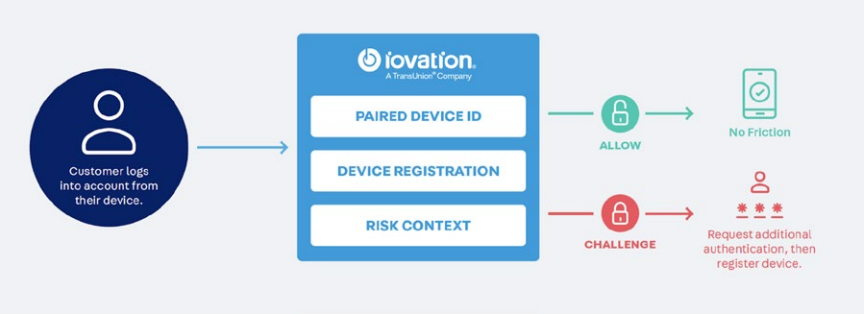
LaunchKey provides multifactor authentication and authorization that is easy to integrate into a mobile app. Merchants can refine consumer login, authentication, and authorization processes with **LaunchKey**, a "friction-right" customer-friendly approach for mobile authentication that reduces the need for high-friction methods such as one-time passwords (OTP) and knowledge-based-authentication (KBA). It allows a merchant's customers to select the authentication method of their choice as well as the devices they wish to link to.

Merchants can also choose the specific types and number of methods that they want their customers to use. This provides control over the types and levels of protection at every type of interaction—for example, by requiring biometric factors (facial and thumbprint recognition) at high-risk interactions like saving changes to contact details or submitting a purchase. **LaunchKey** also fulfills PSD2 requirements for Strong Customer Authentication (SCA) methods with a combination of inherence, possession, and knowledge factors. Specific methods include:

1. **One-touch authorization:** A simple notification that users touch to accept or decline
2. **Circle code:** An interactive "combination" lock
3. **Fingerprint scan:** Uses the device's fingerprint capabilities to authenticate using a user's fingerprint
4. **Facial recognition:** Uses the device's facial recognition capabilities to authenticate using a user's face
5. **Bluetooth proximity:** Authorizes a user's login request based on a linked device's proximity
6. **Geofencing:** The ability to use the geolocation of the user as an authentication factor
7. **PIN code:** Permits numeric-based authentication

ClearKey device-based authentication provides customers with robust, reliable security that's balanced with a seamless, friction-right user experience. Essentially, users register their devices to their account, which allows them to be transparently authenticated on subsequent visits. **ClearKey** device-based authentication provides a transparent second-factor authentication method

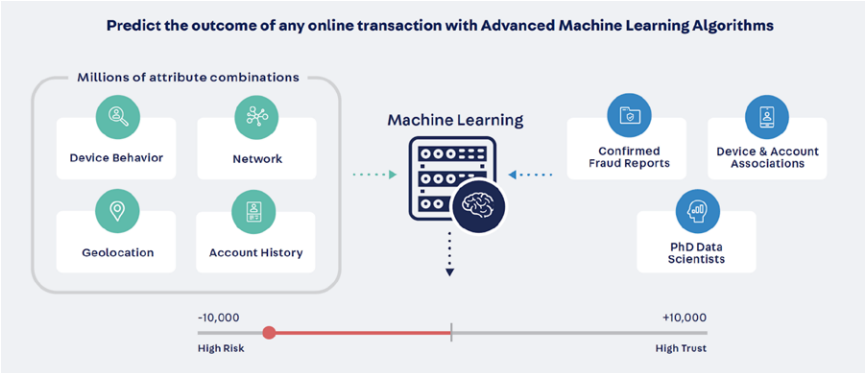
utilizing the customer's paired device via **iovation's** patented device-recognition capabilities. It also provides transaction risk assessments that spot suspicious device characteristics and indicates whether step-up authentication using **LaunchKey** multifactor authentication is necessary. The combination offers an authentication method that is stronger than each solution separately.



The technology uses hundreds of device attributes to instantly identify a device without the need for directly identifying personal data. The technology verifies a user by matching device fingerprints and pairing known good device IDs with the user's account, replacing the need for usernames and passwords or adding a possession factor to existing authentication methods.

A merchant can work with **iovation** to reduce consumer challenges based on acceptable risk: the right friction at the right time. **ClearKey** device-based authentication can show if the device is an exact match, has altered characteristics or risk signals. Based on this, **ClearKey** can drive subsequent authentication and step-up actions. They use elements such as language details, software technology, operating system, browser version, and location of the IP address.

SureScore trust indicator uses predictive machine learning to uncover trusted customers, improve the online experience, reduce transaction review queues, alleviate the need for costly step-ups, and prevent more fraud by exposing hidden risks. It is trained on the 76 million authoritative records of fraud submitted by **iovation** customers, combining the power of both human and machine intelligence. This adaptive, real-time algorithm scores transactions based on subtle behavior patterns. It can detect new fraud trends as they emerge, allowing merchants to stop fraud sooner. But it also helps businesses identify good customers early so that they can make it easier for them to log in, open an account, make a purchase, or take advantage of a promotion.



Email and Phone Verification

As an add-on feature to **FraudForce** device-based reputation, email and phone verification provides an additional vector to test fraud using the consumer-provided email address or phone number (**TransUnion** enhancement, see more on pages 88-93).

Phone number verification assigns a risk score to flag potential risk. The phone number risk score takes into account several indicators, including previous fraudulent activity and other attributes such as carrier, SMS capability, and phone type. It also considers odd traffic patterns, such as a single phone number connecting to accounts in five different languages within the same week, as this may indicate that the phone is being shared.

Email verification enables you to assess risk for an email address before deciding whether to accept it. You can test the email address to uncover if it's valid and functional, how long it's been in use, how frequently it appears on sites across the network, and how popular it is on those sites. These details tell you a lot about whether you can trust an email address. For example, if the address is newly created and its level of activity is unusually great, you may choose to review or deny the transaction—particularly if you correlate the suspicious email activity with other device risk signals such as emulator usage.

Email and phone number verification provide an extra layer of risk insight at critical points including:

- **SMS One-time Passcode:** Before sending an SMS one-time passcode (OTP) to verify a user's identity, assess the risk of the phone number.
- **Account origination:** New emails are commonly used for synthetic identity fraud. Assess the risk of submitted email and phone fields at account creation to distinguish the deceptive fraudsters from your good customers.
- **Account management:** Account takeover attacks frequently attempt to change key contact fields. Check the phone or email details on an account before any account changes are made.
- **Checkout:** Shipping fraud and payment fraud attacks commonly use new email addresses and burner phone numbers. Evaluate the risk of the email or phone number at checkout, especially on guest purchases.

iovation

Services Offered:

iovation's services include two key components:

1. **Customer Success services: iovation's** Customer Success Management team is based across the globe to support their customer base. They offer traditional client services as part of their contracts to customers who are directly integrated with them. As Certified Fraud Examiners, **iovation** Customer Success Managers provide guidance on customers' specific fraud challenges and offer a day-to-day review of client volumes and solution effectiveness as well as quarterly business reviews.
2. **Support: iovation** also offers 24/7 technical support. Clients and the Customer Success Management team can open tickets to resolve any technical issues.

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 is a leading provider of 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 allows 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 customize and adapt their fraud-screening strategy in real time, leveraging best-in-class industry machine-learning models, configurable fraud and policy rules, and robust reputational community data. The platform can perform risk assessments in real-time, in batch, or via manual review, and offers a wide variety of pre-integrated connections to third-party API 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, prebuilt 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:

Case Management: The Interceptas® Platform offers clients an incredibly configurable tool for analyzing, risk assessing, reporting on, and managing 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 2019, **Accertify's** Case Management changes centered on a few key themes, including:

- Improved navigation and User Experience (UX) enhancements.
- Continued investment in industry-focused machine learning models.
- Improved capabilities for managing large fraud teams, focusing on speed and efficiency.

Machine Learning Powered by Dynamic Risk Vectors: Accertify's 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 vs. 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 transaction decisioning outside of business interactions.

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

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** analyzes connected devices to detect known malicious applications as well as criminal tools like location spoofing and IP address proxy apps. Malware files are dynamically updated without client interaction.
- **Rooted/Jailbroken Detection: InMobile** protects against increasing and more complicated rooting methods used by

fraudsters, such as cloaked Root, through Advanced Root and Jailbreak Detection.

- **Certificate Pinning:** Certificate Pinning allows clients to avoid many different attacks by preventing traffic interception between the legitimate mobile app and their server, exclusively connecting to the correct server.
- **Trusted Path:** Trusted Path is **InMobile's** security architecture that 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 codes 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.

Core features include:

- **Device Identification:** 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.
- **Cross-Channel Binding:** Users have a more holistic view of devices when they can correlate data between mobile browser and mobile app on the same device. This allows clients to correlate a single user between channels.

User Behavior Analytics: Accertify offers their clients the ability to track the behavior of their customers' web traffic using their user behavior analytics tool, called **Accertify Beacon**. By analyzing behavioral signals from users as they interact with clients' websites, **Beacon** can help distinguish good users from fraudsters and detect suspicious activity from humans or bots. The tool 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, 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, instead, 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 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 the potential risk, wait overnight for a model or algorithm to be updated or calibrated, or use static, stale rules. Profile Builder monitors, in real-time, 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, thereby easing manual review rates and enabling a more efficient and flexible strategy to mitigate risk.

Chargeback Management: Please see full overview in the Chargeback section of the Paladin Vendor Report.

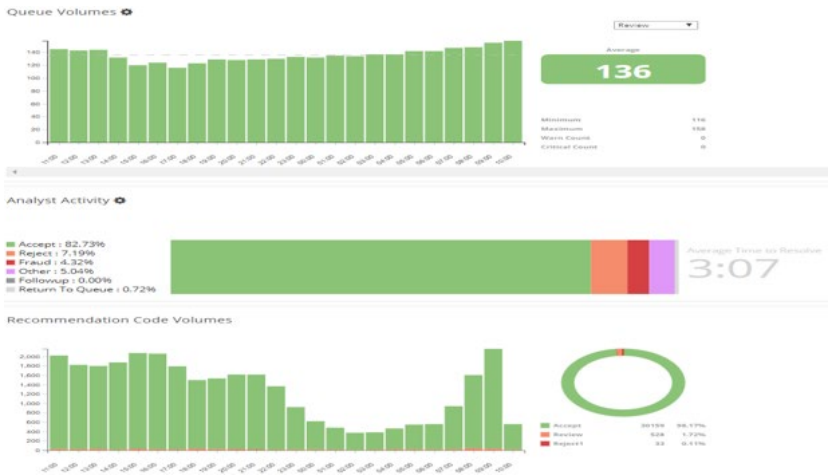
Payment Gateway: This complementary product is for clients seeking a singular platform for payments and fraud. The Accertify Payment Gateway is processor-agnostic, giving merchants the flexibility to select different processors for different payment types. It also provides easy connectivity to multiple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

Accertify, Inc.

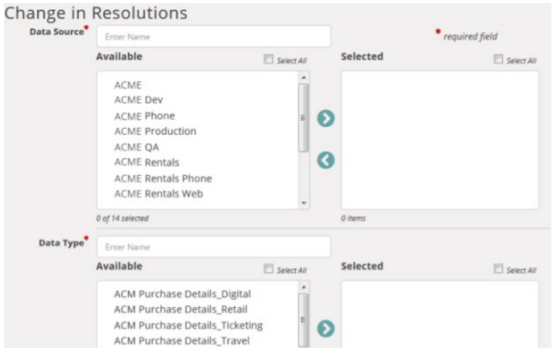
Reporting:

Accertify offers three types of reports:

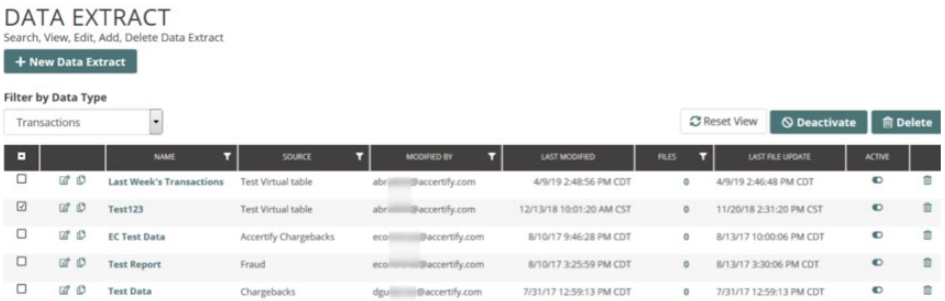
1. **A landing page dashboard:** These are "heartbeat" views of platform statistics—including fraud, chargebacks, and performance—both individually and across the team.



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



3. **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. This can then 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.



Accertify, Inc.

Services Offered:

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

- Building 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.
- Offering full client consultation (Guides) to listen to our client's needs, share insights, and design a set of machine-learning-based solutions to address their needs.
- Research and development pioneering new machine-learning techniques, analyzing new data streams, and other activities to provide our clients with new data insights and predictive risk behaviors.

Client Success Management (CSM): Our global team of Client Success Managers are responsible for ensuring each client is achieving their fraud and chargeback goals. The Client Success Team is primarily comprised of former Directors and Managers of Fraud for the most recognized brands in the world and possess extensive first-hand fraud and chargeback experience.

Accertify's 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. They work with our client base to assist with adoption of these features and functionalities within your environment to achieve the maximum benefit. **Accertify's** Client Success Managers are charged with 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: Accertify's Managed Services team provides direct operational management of clients' fraud and/or chargeback processes leveraging their industry-leading Interceptas platform. **Accertify's** team becomes an extension of clients' organizations by providing experienced and comprehensive consultation, geographical coverage, and SLA management. With **Accertify** Managed Services, clients get the extensive resources they need while driving lower costs and overhead, increasing efficiencies, and gaining peace of mind from knowing **Accertify** has their back.

Support Services:

Accertify's global Support team employs a "follow the sun" approach to deliver white-glove, world-class service 24x7, every time, for every client. The multilingual team has completed rigorous platform and technology training, and they bring to the table their extensive experience in fraud prevention, chargeback management, and client success.

Accertify clients can expect responsiveness, expert consultation, and impeccable problem-solving skills. In addition, through a secure web portal, they offer a rich and comprehensive set of user-friendly support resources to empower clients. This extensive library includes best practices, how-to configuration guides, platform documentation, release notes, and other resources.

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 their 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. Their singular focus is to make clients successful.

ACI Worldwide (ACI ReD Shield)

ACI Worldwide is a global provider of real-time electronic payment and banking solutions to a wide range of verticals and industries. **ACI Universal Payments (UP)** omnichannel vision of "Any Payment, Every Possibility" carries through the company's extensive list of services, including merchant payments, instant payments, transaction banking, online retail banking, and bill payments.

ACI's UP Merchant Payments Solution serves as an acquirer-agnostic "one-stop shop" for merchants who prefer to manage a relationship with a single payments partner, rather than having to establish and manage multiple relationships in order to fulfil their payments processing needs. **ACI** can offer payment solutions with integrated fraud management via a single point of access in the cloud. This provides the high performance and scalability that allows merchants to focus on delivering:

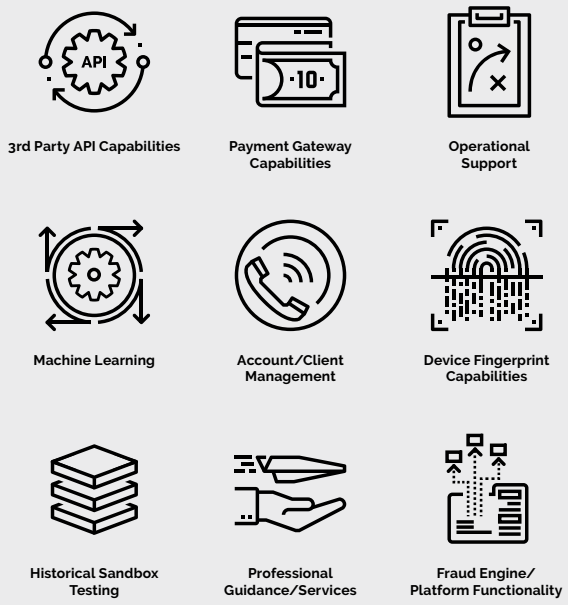
- Increased conversion rates resulting in additional revenue
- Optimized payment acceptance
- Reduced fraud and chargeback rates
- Reduced operational cost

ACI is committed to innovation and continuous solution enhancement—investing 17 percent of revenues each year into research and development. This ensures that **ACI's** technology, services, and advice provide benefits to their base of over 1,500 merchant and banking customers.

Solutions and Functionality

ACI's UP Merchants Payments Solution provides end-to-end payments and risk management services to omnichannel and card-not-present ecommerce merchants

At a Glance:



across a variety of verticals, including telecommunications providers, retail, nutraceuticals, gaming, entertainment, digital goods, travel and hospitality, and Payment Service Providers (PSPs).

Two of the core components of the **UP Merchant Payments** and **UP eCommerce** solutions are the **ACI PAY.ON** payments gateway and the multi-award-winning fraud prevention solution, **ACI ReD Shield**. While **ReD Shield** is fully integrated with the **PAY.ON** gateway, it can also be offered as a standalone solution for merchants who only need fraud prevention. **ReD Shield** can also be integrated via one of its many channel partners. (Additional details related to the **PAY.ON** platform can be found via the Paladin Payment Vendor Report.)

ACI ReD Shield is a multilayered real-time fraud solution that uses machine learning combined with a series of real-time alerts and near real-time dashboards. Fraud strategies are modeled to the requirements of each merchant's needs. **ReD Shield** provides instant automated decisions and supports real-time and retrospective screening on all transactions across all distribution channels, geographies, product types, and payment types. The solution's self-service business intelligence portal, **ACI ReDi**, provides a window into the merchant's transaction data, allowing them to monitor key performance metrics and proactively refine their fraud prevention processes.

A multilayered approach to fraud

As part of the multilayered approach to fraud prevention, **ReD Shield** utilizes machine-learning neural scoring alongside positive and negative customer profiling, blacklists and whitelists, fuzzy matching, IP geolocation, Device ID, and third-party call-outs. These are all underpinned by multidimensional rules, the case management workflow tool, enhanced data responses, and silent-mode rule logic testing. **ACI** also offers vital ongoing support through their global team of risk analysts who help clients configure and optimize their fraud strategies in line with relevant and emerging trends.

ACI works with a hand-picked selection of partners to offer additional support and insight in specialist areas. **ACI** facilitates the connection on the customer's behalf with no exclusivity and utilizes the third-party response within the fraud strategy. This approach adds an additional technology layer, which can further support optimized conversion rates and minimized false positives. Current partnerships include Iovation, Perseus, ThreatMetrix, and Neustar.

Machine Learning

ACI supports and develops multiple machine-learning model options including merchant-specific models (for larger merchants) and vertical-focused models (such as travel, retail, gaming, etc.). The solution's feature set ensures the models are high-performing,

no matter which sector a client is in. With **ACI's** consortium of data, every merchant reaps the benefit of models that have been trained on volumes of industry-specific data. This ensures consistent and reliable performance over long periods.

ACI has brought patent-pending advancements to **ReD Shield** via new incremental-learning algorithms. These models can self-adjust without the need to re-train. These advancements are focused on reducing the need for model replacement while maintaining performance for longer periods without degradation.

Auto-Analyst

ReD Shield offers an auto-analyst function that allows for further automated investigation outside of the real-time window. Questionable transactions can be routed through the auto-analyst function to third parties for additional intelligence, enabling an "accept" or "decline" decision based on the responses. The auto-analyst function can be more heavily used in times of high volumes when the manual review teams are under pressure, or it can fast-track time-sensitive transactions such as "same-day delivery" or "buy now / pick up in store."

Fuzzy Matching

The "fuzzy matching" pattern recognition functionality can help identify linked fraudulent attempts where address concatenation/manipulation and/or email tumbling might appear as unique transactions to most fully automated systems. This allows merchants to more easily spot fraud trends and take fast action to stop it.

Feature Manager

ReD Shield's Feature Manager allows merchants to use its template library to download, configure, and deploy multidimensional and complex rules. A feature incorporates several conditions and calculations in one or multiple fields as one string—such as conditions based on time, product channel, and velocities, plus calculations based on deviations, sum, count, averages, time on file, etc. This provides several efficiencies, not only by removing the need to build rules from scratch, but also by removing the need to have multiple rules when one feature will achieve the same outcome. Users can deploy the feature into rules using a real-time Rule Manager tool or via the **ACI** Risk Team. Templates in the library are all adjustable.

Silent mode for rule testing

Rules are applied to run in parallel through silent mode for a period before applying to active mode (production), for example, champion/challenger strategies. This allows merchants to test the effectiveness of a rule and optimize it without impacting live customer transactions.

Positive Profiling feature

The solution's positive profiling functionality provides additional

visibility into potential high- or low-risk transactions by screening the client's transaction against **ACI's** global consortium, creating transaction profiles on over 100 data points (card, IP, email, etc.). Reviewing this data at the local and consortium levels can increase acceptance rates and reduce false positives.

Business intelligence (ReDi)

ReDi is the business intelligence, dashboard, and reporting tool that provides visibility into all activities within **ReD Shield**. The tool continuously tracks key performance metrics associated with rules, profiles, retrospective alerts, false positives, etc., and can help identify new and emerging high-risk trends. **ReDi** allows users to develop, test, deploy, and monitor rules in active or passive/silent mode. The tool is not only accessible by the **ACI** Risk Team—it's provided to merchants for use by internal business analysts as well. This offers merchants a rule management solution that is designed to be self-service but can be supported by **ACI** Risk Analysts to help guide their fraud strategy where needed.

The **ReDi** application holds two years of transaction history. It provides a host of relevant detail, including volumes, values, and metrics like fraud decline. You can view manual review and acceptance rates, as well as trends on a global and channel basis. All this can be performed hourly, daily, weekly, monthly, and yearly to give useful comparisons on rule performance by measuring chargeback, fraud, and acceptance rates.

In addition, profiling and enhanced response fields can be viewed within the profiling tab in the application. Depending on user requirements, risk rates can also be filtered by BIN (and other applicable banking/payment details). All data is printable and exportable based on characteristics of the order and rule strategy.

The **customer service interface (CSI)** offers merchants a management interface that includes case management workflow functionality. This gives users access to decisioning rationale on individual transactions, including order data points, response, and rule description explanation. Color codes indicate where responses fall in the risk spectrum, which increases visibility into high priority indicators. Third-party callouts are also accessible through the interface, providing manual review staff with additional data insights that assist in their decision-making.

Agents can take action from the interface, applying custom or predefined notes. For example, "cancel" reason codes can drive customer notifications and can give feedback into a reviewer's email server. An audit trail exists in the access log, which provides a quick view of transactions reviewed by agents. Users can be granted unique access levels or can be added to an existing group with preset access levels.

ACI Worldwide (ACI ReD Shield)

Services Offered:

With support teams positioned across the globe, **ACI** offers "follow the sun" customer support. This includes a team of risk analysts covering four continents (and 15 languages) who have access to global payments intelligence and local market knowledge. Agents average five years of experience and many of them are certified ecommerce fraud professionals. All have degrees in math, computer science, or data science. Support can be reached 24 hours a day, seven days a week, 365 days a year.

Merchant customer interaction begins and remains with the Customer Success Manager and designated risk analyst during and beyond integration. Regular meetings are held to review key performance metrics, and recommendations are made to enhance the strategy. Risk analysts are cross-trained and support all verticals, regions, and customer types.

In-depth merchant background is collected, existing processes and operations are reviewed, and a potential solution approach is identified. From there, merchants start to interact with the risk and customer service teams. Once integrated, the single point of contact is the allocated Account Manager (and risk analyst if applicable).

Additional services include manual review support as well as chargeback representment if needed.

Integration:

ACI offers merchants a cloud-based deployment for its e-commerce fraud capabilities. **ACI** also has a large banking customer base utilizing its on-premise fraud management capabilities. The typical integration time frame is six to eight weeks, depending on priority and client resources. The primary point of contact during integration includes a Project Manager and Service Delivery Manager, who are responsible for guiding the integration process and overseeing tasks like issue tracking, identifying friction points in the process, defining fraud strategy, etc.

The initial strategy begins with a historical data dump (using at least six months of data) of all transaction attempts, 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 client, to ensure optimization.

ACI Worldwide (ACI ReD Shield)

In development over the next 6-12 months

ACI is launching an enhancement to the rule manager functionality. This will include the ability to test rules against historical data rather than running rules in silent "live" mode. The functionality builds off the 2018 heavy technical and architectural investment in the solution and serves to expedite rule and model testing and evaluation. Results will be returned in minutes rather than days or weeks (for rules with a time-based element included). In addition, **ACI** will be launching the following updates throughout 2020:

- Data Analysis enhancements to **ReDi** will enable further analytics and pivots advantages within dashboards and exports mass data from Business Intelligence (BI). This will also enhance the stability and speed of dashboard building in a Hadoop (big data) environment.
- Data Analysis enhancements to **ReDi** will enable self-service / self-design reporting.
- Customer profiles will allow merchants to create custom profiles based on individual needs. When coupled with the new Rule Manager and List Manager, merchants can create customized conditions, features, and lists to significantly enhance "allow" decisioning for good customer acceptance and further minimize false positives.
- Additional rule score options will be available to supplement existing machine-learning modelling.
- Data Source improvements will include an improved ability to capture data from sources such as social media, customer authentication tools, and new third-party vendors to further enrich data-mapping capabilities.

Arvato Financial Solutions

Arvato Financial Solutions is a global financial service provider and part of Bertelsmann SE & Co. KGaA as a subsidiary of Arvato.

The company has around 7,500 employees in 17 countries, including a strong presence in Europe, Brazil, and the U.S. They offer flexible full-service solutions for efficient management of customer relationships and cash flows. **Arvato Financial Solutions** is synonymous with professional outsourcing services centering on cash flow in all phases of the customer lifecycle – from risk management and invoicing to debtor management, the sale of receivables, and debt collection. As part of this, **Arvato** focuses on minimizing default rates in the business initiation phase and during the collection process. As a result, services also include optimizing the selection of payment types internationally.

As a financial solutions provider, **Arvato** manages around 10,000 customers, specializing primarily in the retail/ecommerce, telecommunications, insurance, banking, and healthcare sectors. This makes them Europe's third-largest integrated financial service provider.

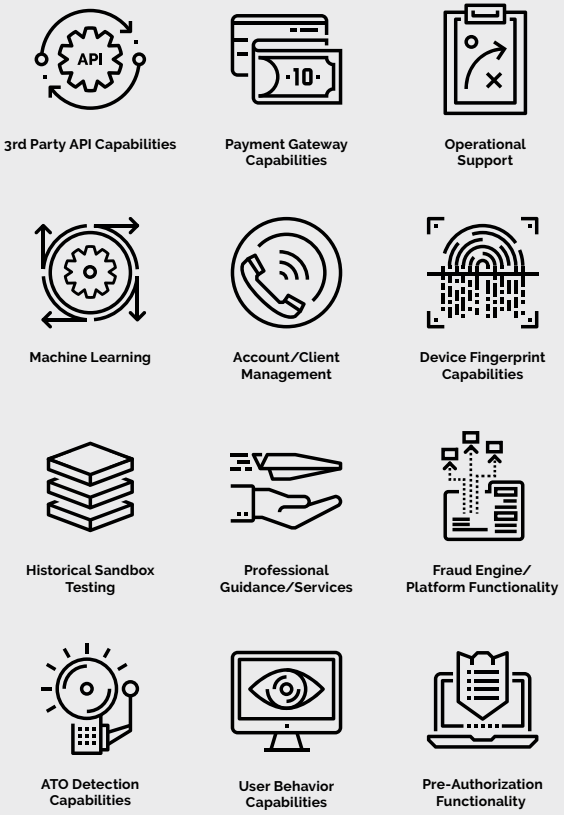
Solutions & Functionality

Within the ID & Fraud Management segment, **Arvato Financial Solutions** offers solutions and services to prevent and detect fraud while allowing an optimized experience for legitimate customers. These services can be applied as an end-to-end solution, or as segmented modules depending on the client's need.

Merchants can utilize the **Arvato Financial Solutions** infrastructure as an approach to new markets as well—for example, when entering the European market with its unique payment and legal landscape. **Arvato Financial Solutions** uses a "make,

arvato BERTELSMANN Financial Solutions

At a Glance:



partner, buy" strategy, bringing together the best technologies with regional, financial, and cross-industry expertise. This approach enhances customer trust and ensures that clients have access to the most sophisticated technology available to fight fraud. **Arvato's** solutions and modules operate in real time and in accordance with European data protection legislation.

These solutions include the following:

Device Fingerprinting helps clients identify and recognize a device based on different attributes such as device type, screen size, and user agent. These are gathered to generate a Device-ID. Specific device and transactional data can be put on client-specific blacklists or whitelists as device history is created. This record allows for recognition even if changes are made in the device itself through browser or operating system updates. The technology can also indicate a user's true geographic location and detect proxy servers which are known to be high risk. The association of diverse data types allows for detecting fraud attempts which would not be identified by a single variant.

Device Fraud Pool (DFP) improves fraud detection by providing access to a large database that makes it possible to compare device and transactional information. This is done on a rule basis along with other numerous records in the pool. It helps recognize transactions that seem valid but have been identified as fraudulent by other clients. The rule-set is industry-specific to make it possible to detect industry-specific fraud. This solution can help detect fraudulent transactions earlier in the process and reduce false positives.

The **DFP** increases the value of **Device Fingerprinting** by sharing device and transactional data as input for the Fraud Rules Engine. These datasets from pool clients remain invisible to other pool clients since no transactional data is shared between the **DFP** clients.

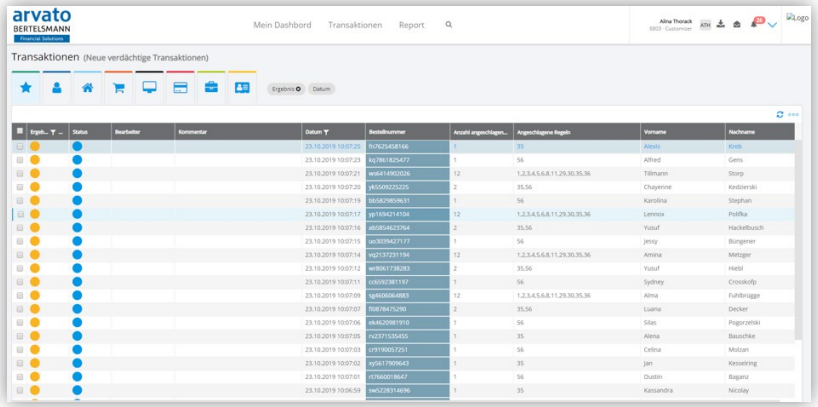
Behavioral Biometrics analyzes device, location, and the user's signals to build an ongoing digital identity. The user is identified based on the individual passive biometric profile (such as user finger pressure, fingertip size, touch coordinates, device movement). The solution also allows clients to authenticate the user's navigation behavior during the web session (such as typing, clicking, zooming, and swiping) against historical and normal population patterns anonymously. This analysis informs clients of fraud risk and gives them advice regarding what actions to take. Not only does this serve to identify high-risk behavior and detect automation, but it also notes legitimate customers' behavior, which can help fast-track good transactions through the checkout process, which reduces potential customer friction. The service is applicable to both web and mobile applications (iOS, Android, Windows).

Arvato Financial Solutions

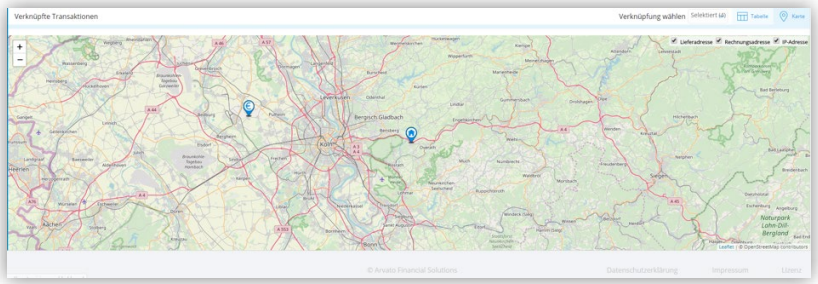
The **Fraud Rules Engine** is a core component of the fraud prevention and detection infrastructure, used to link all relevant data points. It can provide a multidimensional view of data collected, allowing for evaluation of the consumer's transaction. The **Fraud Rules Engine's** design adapts to a number of fraud issues by analyzing correlations on a large set of historical data.

The application of machine-learning algorithms can help complement the rule-based approach, while **Advanced Analytics** also help predict fraud and generate risk scores in real time. In this framework, a recommended action is suggested, and the decision whether to approve a transaction can take place automatically or manually. In conjunction with the **Fraud Management Cockpit**, customers can view triggered rules and manage blacklists and whitelists. Rules can be used across a user base, and the service team supports building new and specific rule sets together with the client.

The **Fraud Management Cockpit** allows clients to manually review transactions based on predetermined rule sets and score thresholds. Transactional data and all fraud check results are displayed in a customizable user interface. The ultimate goal is to provide enough in-depth detail to make a decision, in addition to providing the transparency to follow up on historical judgment without overwhelming the fraud analyst. The optional connection to a client's order-management system allows manual order



review results to be automatically transmitted into the client's order-management system. Examples of features in the response detail include geographical order location, overview of all linked transactions, and order handling recommendations.



Arvato Financial Solutions

Through visualization of connected transactions within the interface, users can apply decisions on orders, add notes or comments, and tab through all relevant customer and order details (such as items, card info, etc.). Linked transactions can be viewed via matrix or linkage map, including potential secondary links. Users can add or remove criteria from the queue that is not relevant, and any changes or customizations to the individual review interface are persistent when logging in and out.

Users can also add or remove "widgets" designed to ingest order detail and track performance of certain rule configurations. Users are then able to search a list of all orders that contain those criteria, which can help track schemes and attacks in either the long- or the short-term.

Arvato Financial Solutions

Services Offered:

To further support the notion of end-to-end fraud solutions, **Arvato Financial Solutions** includes **Fraud Manual Review** outsourcing support among its services. These services are designed for clients who may not have the bandwidth for manual order review, or who may have a seasonal need during peak volume periods.

Arvato Financial Solutions' experienced fraud agents support in manual online fraud prevention with knowledge of country-specific and industry-specific fraud schemes and behavior. Decisions are generally taken directly, but in some ambiguous cases, consumers are contacted on behalf of clients. Thanks to an agnostic approach, it's also possible to fully orchestrate customer-specific tools. Based on the global coverage, the team provides "follow the sun" support 24/7/365 for global and regional clients.

Through their industry and global fraud experience, **Arvato Financial Solutions** can create **Custom Consulting** experiences for customers in need. The portfolio includes project and change management, solution design, and **Advanced Analytics**. **Advanced Analytics** helps identify possible areas for change, utilizing machine learning, artificial intelligence technology and platforms. In this framework, it is possible to recognize patterns, detect anomalies, and produce forecasts to generate recommendations for optimizing financial digital business processes and strategies. Industry insights, international revenue cycle management experience, and benchmarking all serve to support statistical methods and address a number of key performance indicators.

Arvato Financial Solutions' Fraud Management Consulting evaluates fraud models, provides insights and analytical knowledge across all industries.The fraud management is handled through an account team, which can offer process assessment and suggest areas for potential optimization.

Operational and Technical Consulting is also available through **Arvato Financial Solutions'** technical client management and integration team. Project setup, implementation, and process optimization services are offered. They follow up after the implementation phase to monitor and ensure sustainable, positive effects on business. This is often done prior to integration. Training is passed on in order to better handle technical needs in the future.

ClearSale

ClearSale is a global fraud protection firm offering clients the ability to stop card-not-present (CNP) fraud, using proprietary technology coupled with an in-house team of experienced fraud analysts. With solutions that vary from fully guaranteed to performance based, **ClearSale** has five main goals:

1. To mitigate against fraudulent activity.
2. To maximize conversion and minimize falsely declined transactions.
3. To compensate any losses related to fraudulent chargebacks, including "friendly fraud."
4. To create the most seamless process possible.
5. To be fully transparent, ensuring that every step is visible to the merchant.

99% Retention rate

+3k clients worlwide

18+ years in the market

700+ specialized analysts

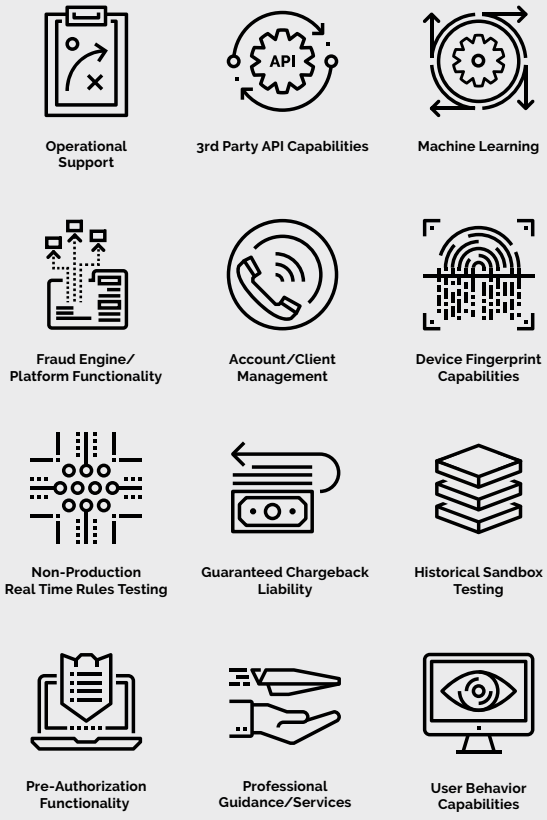
160+ countries

24/7 availability

With over 16 years of experience and a presence in São Paulo, Mexico City, and Miami, **ClearSale** maintains a global footprint. **ClearSale** boasts over 1,500 employees and over 3,000 direct clients, with a 99 percent customer retention rate. Its flagship product is an end-to-end fraud management solution that combines advanced technology software, artificial intelligence (AI) algorithms, and manual review when necessary.

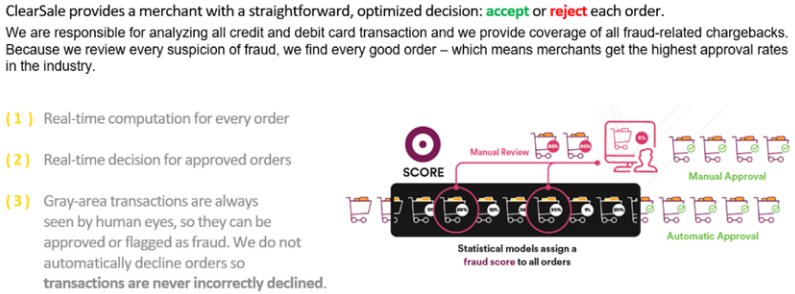
clearsale
Freedom to sell

At a Glance:



ClearSale's solutions are available for transactions placed via web, mobile, and telesales. They use machine learning to help determine fraud risk level and to help quickly approve cleared transactions. If a transaction is deemed to be potentially fraudulent, it's closely reviewed by experienced analysts trained to spot the nuances and understand the context of fraud that machines cannot resolve.

Solutions & Functionality



ClearSale relies on a proprietary machine-learning technology with custom rules and models that are updated continuously and highly customized to various industry segments, and in some cases, for specific customers. **ClearSale** also has a proprietary case management system that enables custom workflows, different data integrations, and third-party integrations. Machine learning breaks down transaction requests into patterns, while looking for abnormalities based on the following criteria:

- Information contained in the order
- Device information
- External data sources
- Behavioral information
- Historical information
- Clusters of similar orders
- Biometric information

When transactional discrepancies arise, **ClearSale's** team of experts conduct a manual exam of order details and information collected. If needed, the analysts will use contact information linked to the cardholder to conduct verifications. Essentially, an order is never declined without a manual review—which is the reason the manual review staff makes up about 70 percent of the company's workforce.

ClearSale's approach limits friction in the purchase process. Manual reviews are only performed for the types of cases that would normally be automatically declined by tools that rely solely on machine learning. **ClearSale** takes the machine learning process, then applies the manual review layer, further reducing the likelihood that a good customer is declined.

ClearSale's Mission has five main objectives:

1. Prevent fraudulent activity: **ClearSale** originated in the dynamic ecommerce environment of Brazil 17 years ago—and their experience in high-risk markets has allowed the company to develop processes that find and mitigate against fraudulent tactics.
2. **Maximize conversion and minimize falsely declined transactions: ClearSale** recognizes that false declines are a very large problem, not only for lost revenue but also lifetime customer value. While the company relies heavily on artificial intelligence to detect fraudulent orders, they also recognize that full automation can lead to increased false positives. Because of this, all flagged orders are sent to in-house review, where analysts complete the investigation manually.
3. **Compensate any losses related to fraudulent chargebacks, including "friendly fraud":** To allow merchants to focus on core competencies, the **ClearSale** process helps merchants reduce concern over the costs associated with chargebacks. Through this process direct chargeback costs can be lowered or altogether eliminated.
4. **Create the most seamless process possible:** From the perspective of the customer, the transaction is already completed and there is no extra action needed (transactions are shown as "Pending" in the merchant's back-end until they are verified). The customer experience is maintained, with a reduced likelihood of losing good customers to bad fraud filters.
5. **Be fully transparent, ensuring that every step is visible to the merchant:** To be an integrated part of a merchant's team, **ClearSale** provides merchants with access to a dashboard via PC, tablet, and smartphone—all of which allow the client access to real-time data related to:
   - Pending approval requests
   - Current approval rate
   - Response time
   - Recent orders
   - Activity history for current day, last week, last month, and last year
   - Details of specific orders and how they relate to other orders

In addition to the online dashboard, clients have access to data insights reporting with detail ranging from macro- to microlevel. **ClearSale's** technology is not a black box as others are; all information is available to merchants, empowering them to make the best decisions for their business.

Service level agreements are typically based on chargeback rates, approval rates, and turnaround time, and custom ad-hoc KPIs are available based on unique merchant-specific scenarios.

Pricing:

ClearSale's pricing is based on each client and their unique needs. Each price structure considers the benchmarks, KPIs, goals, and ROI for the business. From this, a custom-tailored price point is created. In general, **ClearSale** offers two performance-pricing models. They are similar, but have a few key distinctions:

- **Total Guaranteed Protection Solution:** 100 percent reimbursement of fraud-related chargebacks. With this, there is no risk—if a merchant runs into fraud, **ClearSale** will cover it.
  - The merchant pays a fixed percentage on approved transactions.
- **Total Protection Solution:** For every chargeback, versus the target, **ClearSale** will offer a discount on the service.
  - The merchant pays a fixed fee for approved transactions.

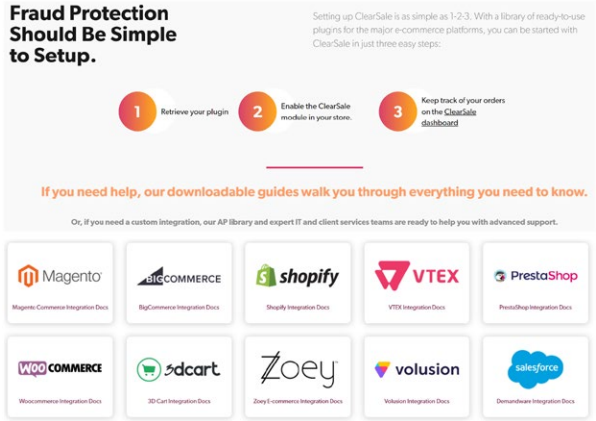
Support Offered:

ClearSale offers the following **integration/support** to its clients:

- **Direct integration:** Can be managed by the merchant through the **ClearSale** API library and client service team. Integration is simple and seamless, with custom API options and direct support.
- **IT Consultant:** During the integration process, each customer is assigned an IT consultant. Post integration, 24/7 IT support is available through phone and/or email.
- **Account manager:** After go-live, each customer is assigned an Account Manager. 24/7 support is available through phone and/or email.

System Integration:

Clients of major platforms (such as Magento, Prestashop, Shopify, WooCommerce, BigCommerce, etc.) can integrate in three steps:



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

The average integration time is eight hours if a merchant follows the API guide, and one hour if installing via one of the platforms' plugins (Magento, Shopify, etc.).

Security:

ClearSale understands that security is important, especially in today's climate of increased cyber attacks and data breaches worldwide. **ClearSale** has never had a data breach or faced any potential security risk and protects its data with the most advanced data protection technology.

ClearSale processes all data pursuant to all laws, regulations, and other binding legal sources governing data privacy and security. This includes the EU regulation General Data Protection Regulation 2016/679 (GDPR). **ClearSale** has implemented technical and organizational measures for data protection, including measures to protect against accidental or unlawful destruction or alteration, unauthorized disclosure or access to any client's raw data. **ClearSale** protects the security, confidentiality, and integrity of the information provided to **ClearSale** by its clients.

Required information includes:

- Card type
- Card's first 6 digits
- Card's last 4 digits
- Expiration date
- Billing address

CyberSource

CyberSource is a California-based, Visa-owned company founded in 1994. They offer payment gateway services as well as a variety of card-not-present risk management and mitigation solutions. **Decision Manager (DM)** is their flagship enterprise level risk management solution. It combines fifteen region-specific, channel-specific, and industry-specific machine-learning risk models (each optimized to identify fraud in different scenarios) with various detection tests, a fully customizable rules engine, case management capabilities, and real-time reporting. **Decision Manager** helps merchants find a balance between maximizing revenue, reducing fraud losses, and controlling costs. With unique insights from over 68 billion transactions that **CyberSource** and Visa process annually worldwide, **Decision Manager** has access to a massive data consortium. From this, it pulls high- and low-risk signals from across the network to provide industry leading detection.

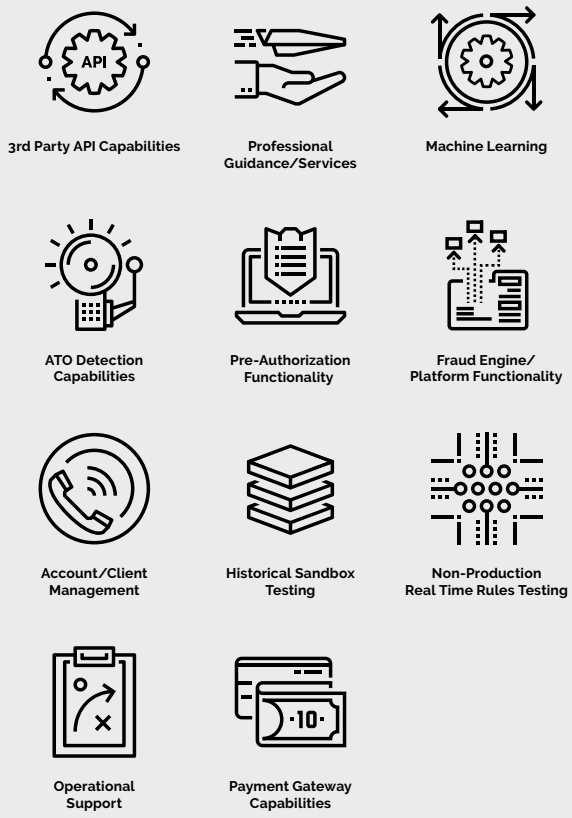
In addition to **Decision Manager**, **CyberSource** is introducing Fraud Management Essentials, a new simple, flexible and robust fraud prevention solution designed for small to midsize businesses.. Fraud Management Essentials leverages the powerful machine-learning risk models of **Decision Manager** to provide a transaction risk score along with a set of configurable rules, list management, and order review capabilities.

Decision Manager Solutions & Functionality

Once integrated, the **Decision Manager** fraud platform provides machine-learning results on all transactions processed. This is most commonly used by merchants in the form of a score (from 0-99), but the platform also returns indicators that provide in-depth insight into the results. Users may also configure and manage fraud mitigation processes through a customizable rules engine, without additional IT resources. The platform utilizes both static and dynamic machine-learning technology designed to enhance

CyberSource®

At a Glance:



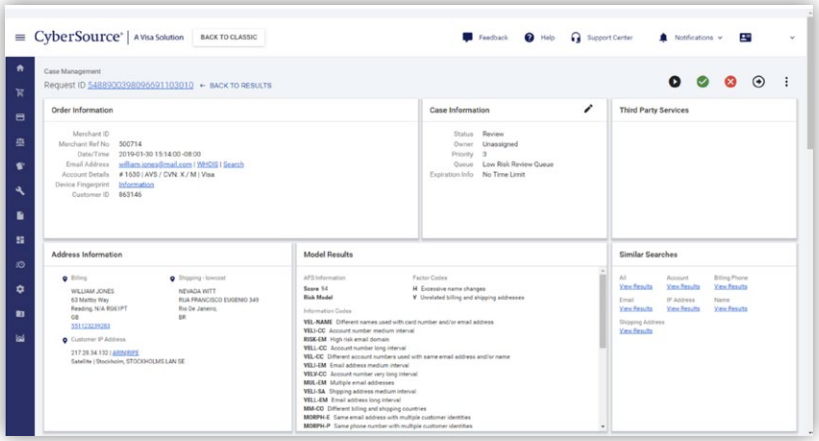
the capabilities of their rules engine. The solution offers more than 260 automated validation tests and draws insights from more than 68 billion worldwide transactions processed annually by Visa and **CyberSource**.

Identity and behavior tracking results are included via **Decision Manager's** machine-learning platform. Some potential results included currently:

- Information on excessive address changes—for example, if the customer changed the billing address multiple times or used multiple credit cards in a certain time frame.
- Tracking of identity-morphing behavior: **DM** can find multiple values of an identity element that are linked to a value of a different identity element—for example, if multiple phone numbers are linked to a single account number.
- Detecting velocity-based behavior, for example, including alerts if the customer's account number was used many times in the past 15 minutes, **DM** also can expand on velocity behavior by providing global validation of specific velocity use, such as account number, email, addresses, IP address, all being used in a short, medium, or long tracking interval.
- Behavior surrounding customer input is collected and analyzed, and it can provide details such as nonsensical input, repeated characters, and input data.

When needed by a merchant, **Decision Manager's** case management system facilitates the manual review process by bringing together information and tools into a customizable, unified interface. This allows review staff to evaluate transactions based on **Decision Manager's** assessment of fraud risk, and it gives staff access to rule strategy outcomes and data points indicative of the associated risk. Additional benefits include:

- Harness callouts to third-party validation services such as Whitepages Pro and Emailage, Perseuss, and Creditlink.
- In-depth review process and user privilege control, allowing added layers of security and process flow management (e.g., service level agreement triggers, permissions, etc.).
- Data that is exportable into a merchant's own case management system.
- Configurable screen workflow and localized language.
- Administrative access to performance metrics for each reviewer.
- Direct integration with the ThreatMetrix Device ID functionality.



Decision Manager includes multiple platform-based data providers, including built-in device fingerprinting. Merchants who take advantage of device fingerprinting do not pay extra for this service, and device-based results are immediately available in rules, configuration elements, and in the machine-learning results.

For rule and model management, **Decision Manager** lets users construct rules by using a predefined library of default rules broken out by category—and by using a custom rule-builder allowing for over 40 transactional criteria.

Through third-party partnerships, rules can be designed to interact with multiple global validation services for enhanced authentication. Users with a business need can build multiple screening profiles based on product category, SKU, country, channel, etc. Default predictive models are available based on region and industry. Merchants with variable transaction volume throughout the year have the ability to roll out or revert rules for specific periods, such as peak season.

When it comes to reporting, **Decision Manager's** interface offers a number of real-time options for performance monitoring and management, including financial impact, system reports, and review team performance.

The combination of machine-learning results and rules is possible with this system. For example, a merchant can create a rule that takes a score threshold and uses it alongside other order attributes (for example, if the score is greater than 80, and billing address doesn't equal shipping). This flexibility allows merchants to control the **CyberSource** predictive results and support business policy at the same time.

Pre-Authorization Transaction Screening through **DM** runs **DM** 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 **DM** prior to authorization also enables Payer Authentication results within **DM's** rule-building capabilities.

Merchants can also integrate Payer Authentication as a full component platform service. Enhancing the integration for Payer Authentication (Cardinal Commerce) as a full component service

allows **DM** rules logic to dynamically call payer authentication as part of the risk and optimization calculus. Merchants can now combine their own risk assessment in the context of how that transaction would be treated by the Issuer (e.g., VCAS, not participating, etc.). This maximizes 3D Secure benefits to merchants without compromising the customer experience.

The **DM Account Takeover** (ATO) functionality allows merchants to monitor for suspicious activity at several potentially high-risk touchpoints like account creation, account login, and account updates. Users can proactively monitor and secure customer accounts from unauthorized use. The service helps merchants distinguish between high- and low-risk sessions. It works with any payment platform and integrates with **Decision Manager**, allowing users to build rule layers associated with these behaviors and prompting for manual review or reject (in the case of high risk), or auto-accept (in the case of low risk).

The **CyberSource Rules Suggestion Engine** uses the outputs of **Decision Manager's** machine-learning models as inputs into the rule creation process. The **Rules Suggestion Engine** draws on a merchant's unique transaction history to automatically present recommended rules that can augment existing fraud strategies. Each rule is accompanied by appropriate metrics to help merchants measure its performance against the selected transaction data. This functionality can be especially useful in combination with **DM Replay**, which can help confirm the future value of a rule or rule set.

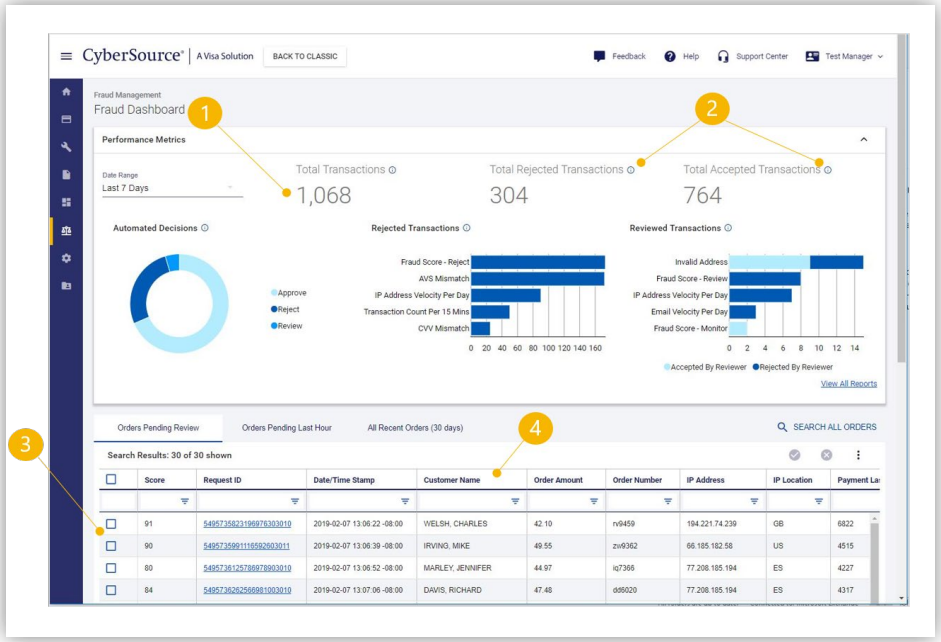
DM Replay testing functionality allows merchants to quantify fraud strategies in real time prior to activating in the live production environment. The format is essentially a "what-if" testing function that uses a merchant's own historical data, retroactively applied to a new rule or model. The real-time reports return likely changes to the review rate distribution and fraud rates.

Finally, with **CyberSource Fraud Alert**, merchants receive notifications in near real time—as soon as fraud is confirmed by the issuing bank. By receiving email notifications directly from the issuer, merchants can avoid some of the inherent delay in the chargeback process. This allows expedited processing and potentially increases the number of chargebacks prevented. Settings allow customization in type and timing of receipt as well as number of users receiving alerts. This function can be set up as a standalone service, usually in under 48 hours.

CyberSource offers a chargeback guarantee product with which (rather than the client being responsible for fraud losses) clients will receive a credit from CyberSource for chargebacks reported as fraud. For this product offer, the client is charged a percentage of the value of all accepted transactions. The client is not charged for rejected orders.

Fraud Management Essentials Solution & Functionality

A lightweight and powerful fraud prevention tool that is designed to meet the needs of small to mid-market businesses. Merchants can focus on their business knowing they have the scale, security, and analytics of Visa and CyberSource helping to protect them from card testing, payment fraud, and common abuse scenarios while enabling them to grow from micro to enterprise on a single platform. Merchants can utilize the automation of machine learning while retaining control over their own risk tolerance. They can choose to enable a few rules or no rules, and choose to review no orders or all risky orders.



Included with Fraud Management Essentials:

- Dashboard with rule performance and decision insights.
- A risk score generated by **Decision Manager's** comprehensive machine learning platform.
- A configurable risk score slider to configure the decisions to match the merchants risk tolerance.
- A set of configurable standard rules, geo-location rules, velocity rules, and threshold rules.
- Preconfigured fraud settings (adjustable).
- (Optional) fully automated, real-time decisions.
- (Optional) manual review capabilities.
- List management (negative, positive, & review lists).
- Order search, similar search, & data visualization.

Services Offered

CyberSource's Managed Risk Services program offers merchants a range of service options, from consulting and monitoring to complete outsourcing of manual review, with 24/7 global coverage. The teams work with merchants to identify new fraud trends and schemes before they impact the business. With teams located on six continents, they have deep local knowledge and experience. This function can help merchants scale to increase growth levels and/or handle seasonal volume fluctuations. It can also be helpful as merchants build fraud strategies when considering expanding into new geographies, markets, and channels.

CyberSource offers three levels of service, all of which include customized reporting.

- An assigned Risk Analyst actively manages fraud 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—this can include overnight hours, peak season, and high loads during special promotions.

Additional benefits include:

- Regional teams with local knowledge serving six continents.
- Managed risk analysts with fraud expertise from the merchant's industry.
- Outsourced fraud operations service (automated screening and manual review).
- Ability to use for all operations or selected markets, or for peak volume overflow.
- Includes performance monitoring services plus a team of review experts.
- Global 24/7 coverage.
- Performance metrics and service level agreement negotiated directly.

In development over the next 12-18 months

Identity Behavioral Analytics: A methodology of tracking transaction activity through identity usage and creating individual identity activity profiles. It attaches chargeback data and merchant decisions to that activity, which assists in accurately differentiating good and bad behavior—and helps respond faster to the activities of reviewers. This functionality forms the next significant advancement to the **Decision Manager** machine-

learning system, improving both the models and enriching the data available for rule-building.

It can help merchants identify different types of identity patterns and is designed to improve **Decision Manager's** ability to reduce false positives by profiling good customer behavior more accurately.

PSD2 SCA Automation: CyberSource intends to incorporate automatic SCA exceptions such as transaction value, merchant positive listing, mail order telephone orders, corporate card transactions, and other criteria–challenging only the transactions that present a higher risk and thus require a challenge be sent.

Visa Transaction Advisor (VTA) will also be supported in **Decision Manager** as a third-party provider with a direct integration available. **CyberSource** merchants will be able to use VTA to identity transactions which will be eligible for exemptions under SCA regulations.

Also of note, Visa has also acquired **Verifi**, a leader in technology solutions that offers dispute resolution capabilities. There will be three main products made available as part of the acquisition. **Order Insight (OI)** allows merchants and merchant facilitators the ability to share receipt-level purchase details with issuers prior to the issuer raising a dispute. **Cardholder Dispute Resolution Network (CDRN)** is a network used to connect multi-network issuers to merchants to resolve disputes (via sending a notice with an intent to credit). Finally **Chargeback Representment (CBR)** is Verifi's fully outsourced dispute management program

Kount

Kount is a leader in digital fraud prevention, using advanced artificial intelligence (AI) to serve 6,500+ customers globally across industries, business sizes, and geographies. Founded in 2007, **Kount** has pioneered the use of machine learning technologies in digital fraud prevention and holds 30+ patents. **Kount's** next-generation AI helps businesses achieve a successful balance between accurate fraud prevention and business-driven outcomes, including positive customer experience and increased sales with reduced false positives and manual review rates.

Kount's Identity Trust Global Network links trust and fraud related signals from more than 6,500 global customers, 50 payment processors and card networks, and 32 billion annual transactions, combined with the decisions from thousands of fraud analysts, to deliver accurate identity trust decisions. With the **Identity Trust Global Network**, **Kount** helps customers establish identity trust levels behind each transaction, login, and account event.

In every interaction, historical fraud data is analyzed with supervised machine learning trained on **Kount's Identity Trust Global Network**. **Kount's** unsupervised machine learning uses advanced algorithms and models to detect anomalies and emerging fraud on a more accurate and scalable basis than human judgment alone. With an incredibly large network of trust and fraud signals combined with adaptive AI and machine learningL, **Kount's Identity Trust Global Network** can uncover the true level of trust behind interactions where other solutions often miss fraud, create false positives, or add unnecessary friction due to limited datasets and lack of real-time AI. This combination delivers powerful and accurate results so businesses can make immediate decisions to block fraud in real time and to enable personalized customer experiences.

Kount®

At a Glance:

The **User Experience Engine** is a key part of **Kount's Identity Trust Global Network**. It enables automated decisions and reduces manual reviews on one side, while on the other, allows the flexibility and control to fine-tune user experiences through customizable policies and rules. Real-time identity trust recognition allows businesses to personalize user experiences across the spectrum of identity – from frictionless VIP experiences to blocking fraud.

Kount's solution enables businesses to distinguish, segment, and address specific types of fraud so that they know where there are gaps in operational efficiencies. The first step in the process is to reduce criminal fraud using advanced AI. Once criminal fraud is under control, **Kount** has a solution to isolate and address incidents of *friendly* fraud. Friendly fraud—an area of fraud growth that has expanded in recent years—requires a specialized set of tools that is typically not included in traditional fraud detection solutions. The ability to quickly and accurately identify and segment both criminal and friendly fraud can mitigate fraud challenges and improve business operations that result in increased revenue.

Kount's AI-driven fraud prevention solution empowers its customers to significantly reduce the time spent on manual reviews so that fraud analysts can focus their expertise on higher-level strategic business objectives that generate growth. The accuracy of **Kount's** AI, combined with its flexible and user-friendly policy engine and control center, allows businesses to manage fraud, chargebacks, and decline rates.

Solutions and Functionality

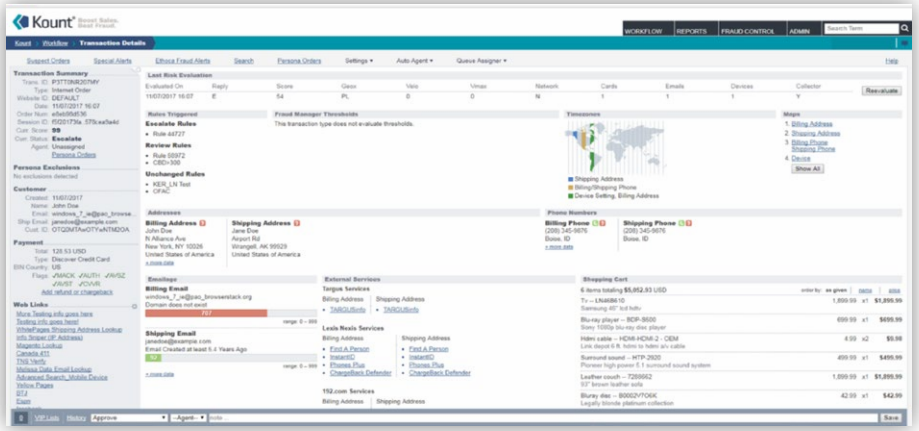
Kount Complete™ was built for online merchants, digital businesses, and enterprise-level retailers. It protects against digital payments fraud, helping businesses reach desired business outcomes around chargeback and decline rates, as well as operational costs. It is the industry's most comprehensive, all-in-one solution that reduces fraud, protects digital businesses, and increases revenue.

Kount Complete is powered by **Kount's** AI, the new frontier of AI-based fraud prevention that protects digital businesses from common and sophisticated fraud attempts. Trained to recognize patterns that have not been seen before, it detects complex and automated fraud in milliseconds.

Running dynamic supervised and unsupervised machine learning in parallel, **Kount's** AI quickly detects anomalies, provides link analysis, and automatically evaluates and weighs features to identify different types of fraud. **Kount's** AI produces Omniscore, an actionable fraud payments score that simulates the judgment of an experienced fraud analyst. Businesses use the highly predictive score when decisioning orders to reduce manual

reviews and a reliance on policies that react to fraud that has been seen in past instances.

Kount's configurable user interface (shown in the next diagram) offers several different views, including a transaction details screen with tabs designed for workflow, reporting, fraud control, business intelligence, and administration views. It offers flexibility related to view options. For example, a quick-view option allows fraud agents to focus on essential transaction details that aid in rapid decision-making.



User Defined Fields: User Defined Fields (UDFs) are a **Kount** feature that help businesses capture details from internal order management systems to analyze orders and make improved and more automated accept/decline decisions. With more than 500 customizable fields, businesses can capture information that is specific to their products, customers, or goals. This translates into data essential for understanding who their customers are and gaining a clear picture of transactions.

Reporting: Fraud prevention managers and analysts rely on Kount's data analytics tool, **Datamart**, to gain deep intelligence into the fraud that is specific to their business. For example, **Kount's Datamart** takes the rich data from payment transactions, customer interactions, and outcomes, and puts them into the hands of businesses to provide insights into business performance. This targeted information helps businesses pinpoint areas for improvement that enhance operational efficiencies, such as customer experience, margins, and revenue.

Kount's Digital Account Protection prevents fraudulent activity for high-volume logins, account creation, and affiliate networks. It identifies fraudulent behavior at login prior to account access or even at account creation. **Kount's Digital Account Protection** protects businesses against account takeover and at account creation to prevent brute-force attacks and multiple account creations.

Kount Central™ is a comprehensive 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 proven AI-driven fraud prevention that uses supervised and

unsupervised machine learning to increase revenue streams and provide additional value-added services. **Kount Central** customers include Chase, BlueSnap, and Braintree. With a single integration, Payment Service Providers (PSPs) deliver a diverse portfolio of fraud prevention services and use cases.

Customer Success Managers deliver personal and immediate support to Kount Complete customers, including:

- Product integrations and business setup
- Conducting day-to-day operations and Level I support (if required), which includes business policy creation and client-specific questions
- Access to the Data Science team, Data Analytics team, and third-party partners for expanded services

The Customer Success Manager works with the fraud team on education, strategy development, business policies, and training.

NS8

NS8 was founded in 2016 by a team with a wide range of experience in online advertising, fraud mitigation, analytics, and scoring engines. They combined forces in an effort to develop a solution that can solve the problem of potential high-risk behavior at the front end of the internet traffic.

They work to answer the questions: Why am I experiencing fraud? What type of traffic and behavior is indicative of fraud? And, how do I cut it off at the source? They are currently integrated with over 5,000 merchants, with increased interest from financial services.

By partnering with a number of popular ecommerce shopping carts, they are providing a platform-based solution that can be easily installed through a direct integration. It focuses on democratizing ecommerce risk mitigation for a wide range of verticals and industries against a variety of risks. The solution is built to meet the needs of most simple organizations but with the power to also support more sophisticated enterprises.

Rather than requiring a long ramp-up or machine-learning period, the **NS8** solution was built to begin solving many fraud issues on day one.

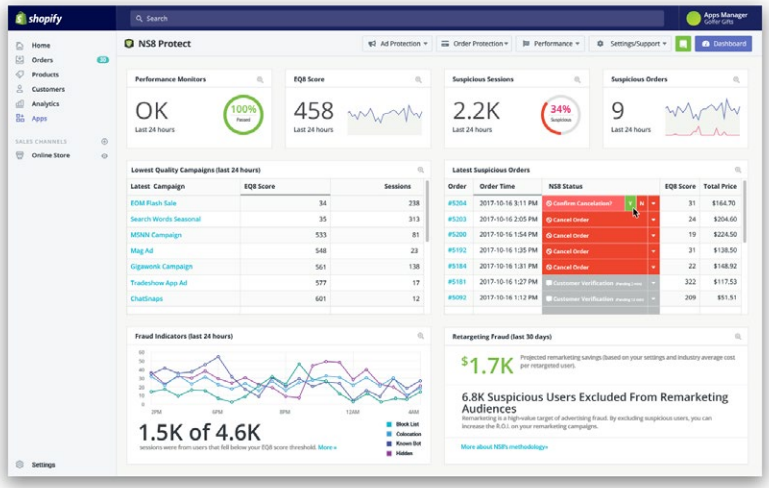
NS8 has made significant progress on several fronts in the past year, with growth of their global team of 500 percent to over 100 employees, and with growth of their customer base to include users in 51 countries.

At a Glance:

Services & Functionality

NS8 defends against online fraud and offers better insight into real customers by utilizing behavioral analytics, real-time scoring, and global website performance monitoring. The solution allows merchants to minimize risk, automate fraud management more effectively, and realize savings throughout the customer lifecycle. **NS8** is currently available in two formats:

- The first is a no-coding plug-in available on seven ecommerce platforms: Shopify, Shopify Plus, Magento, PrestaShop, WooCommerce, thirty bees, and BigCommerce. After installing the plug-in from a platform's app store or marketplace, a merchant can begin collecting data and implementing fraud prevention measures within minutes.



- In addition to the plug-in, stand-alone scoring is also available. This integration option uses NS8's API, and it allows for additional use cases of **NS8's** patented scoring technology that assesses 170 attributes from first click to checkout.

Once the **NS8** tracking script is present on a business's website or mobile app, any application can take advantage of their scoring and analytics solution. An actionable score can be returned in less than 30 milliseconds, with third-party data callouts also available with some extensions. Such a callout could allow an automatic step-up to two-factor authentication or data validation.

Additional use cases for **NS8's** API include payment service providers and gateways, credit applications, account creation and takeover, affiliate and promo abuse, logins, transactions, advertising, and fake accounts.

Payment service providers and gateways, for instance, have products focused on checkout data. **NS8** brings pre-session and user behavioral data to go beyond what is currently monitored in their field.

The graphical user interface displays up to 170 attributes. **NS8's** advanced rule engine allows merchants to build processes and automation best suited to their individual businesses. Every evaluation screen allows a merchant to choose the relevant fields

they want displayed, and they can download the data for analysis with other tools.

Rules are built by clients directly in the interface. Rules and the resulting automation can be built based upon a majority of the 170 attributes that **NS8** tracks and third-party extensions. **NS8** support is available for consultation, as needed, to help merchants configure rules and automation results.

NS8's data cohort is built to leverage activity across the entire network, and it can factor that into scoring without the need for individual shared files.

Reporting

NS8 offers a robust suite of dashboards for identifying suspicious orders, scoring advertising campaigns, and performance monitoring. Within the dashboards, merchants will find such useful metrics as risk scores for transactions and campaigns, insights on suspicious sessions and fraud indicators, and information on conversion rates and revenues.

In addition, they offer reporting that can help monitor site activity—including uptime, security cert expiration, and more. Users can gauge performance of ad campaigns and can score all traffic through those campaigns. Reporting can be processed by data download or via API. The tool also provides for a Google Analytics integration that allows businesses to block low-quality users from retargeting campaigns.

Additional differentiators

NS8 has capabilities to defend against multiple forms of fraud and threats. By offering the integration of multiple threat vectors in one platform, **NS8** has an advantage in being able to link threats. For example, an ad campaign that drives both ad fraud and transaction fraud can be spotted. **NS8** also scores actions earlier than most competitors by not only reviewing payment information and user behavior, but also reviewing pre-session data and noting how the user came to the site. This allows for deeper fraud analysis profiles.

The application of behavioral analytics and identity verification is universal to merchant verticals. Merchants can build rules specific to their business or vertical.

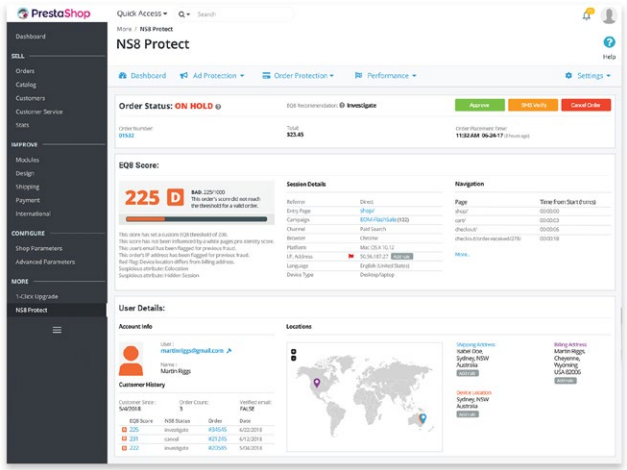
Pricing format

NS8 is a pay-as-you-go service, with tiered pricing based on a store's traffic and no additional service or maintenance fees. Traffic is defined as the total number of orders and page views analyzed on a website in a given month.

Discounts are available for high-volume customers, as well as for customers who elect to purchase annually.

Integration

NS8 can be integrated with any internet situation where a risk score is needed, so long as its tracking script can be deployed and the application can request a score. Additional attributes can be used to segment audiences by risk, device type, or many other criteria.



It takes only minutes to get set up when using **NS8's** integrations. When leveraging **NS8's** API, it typically takes two to five days for the service to become fully functional.

Most merchants choose to install **NS8** and begin using the product immediately for building rules and automation during a startup phase. However, **NS8** can be installed and used to gather information before being set in a live mode during a trial phase.

Support

Basic support is available via phone, online chat, and email, and is included at no additional cost. **NS8** offers new merchants a product consultation with its customer success specialists to ensure that they gain immediate familiarity with our products. Additional professional services are available at an additional cost.

In development over the next 6-12 months

NS8 will advance its platform with major upgrades in infrastructure and ease of integration. They will also incorporate significant enhancements in key functional areas of software, including expanded third-party extensions for user identification and verification and enhanced services for chargeback management.

Sift is focused on digital trust and safety, empowering businesses of all sizes to protect themselves from fraud while growing revenue. Some of the largest digital companies in the world—including Twitter, Airbnb, and Wayfair—trust **Sift** to help deliver positive customer experiences while preventing fraud. With sophisticated technology, a global community of fraud-fighters, and a commitment to long-term partnership, **Sift** helps its customers gain competitive advantage in their respective markets.

Solutions & Functionality

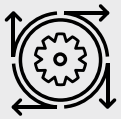
The **Sift Digital Trust and Safety Suite**, powered by real-time machine learning, assesses risk of all live events taking place on desktop and mobile applications across its global network of customers. With over 34,000 sites and apps on the platform, **Sift** customers benefit as the solution collects,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

Sift produces real-time scores for every interaction along the user journey, including account creation, logins, orders, content posting, and any custom events along the way so merchants can make instant and accurate decisions. By taking a holistic look at user's journey, **Sift** is able to detect multiple types of fraud (payment fraud, fraudulent content, account takeover, promotion abuse, and fake accounts) and can identify trusted users.

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 findings about new, emerging fraud patterns across the network, boosting prediction accuracy by up to 30 percent. These are blended with custom

At a Glance:

3rd Party API Capabilities


Machine Learning


Pre-Authorization Functionality


Account/Client Management


User Behavior Capabilities


Fraud Engine/ Platform Functionality


ATO Detection Capabilities


Device Fingerprint Capabilities

models that adapt to each business' specific use case to uncover the fraud patterns unique to them. **Sift** also does extensive feature engineering on individual data pieces to generate tens of thousands of signals across identity, device, behavior, and transaction vectors. This all happens within milliseconds, and merchants are able to take instant action to automatically block or accept transactions, or to dynamically add or remove friction from the user journey.

Sift's products are flexible and can serve as either the primary fraud tool or as an input to a larger, layered approach. Customers can access their data and results through APIs and a customizable web-based console. The console gives trust and safety teams of all sizes a tool to investigate fraud patterns, automate decisions, and analyze business performance. It also supports capabilities for more protection and growth with apps such as multi-factor authentication and false positive experimentation.

Sift offers a full suite of fraud and abuse products in its Digital Trust & Safety Suite. Each product is powered by its own set of use-case-specific machine-learning models and scores. All products are enabled through a single integration and are accessible through the web-based console. Products include:

Payment Protection

- Proactively stop fraudulent chargebacks and protect revenue.
- Streamline operations and reduce manual review.
- Grow revenue with decreased false positives and increased conversion.

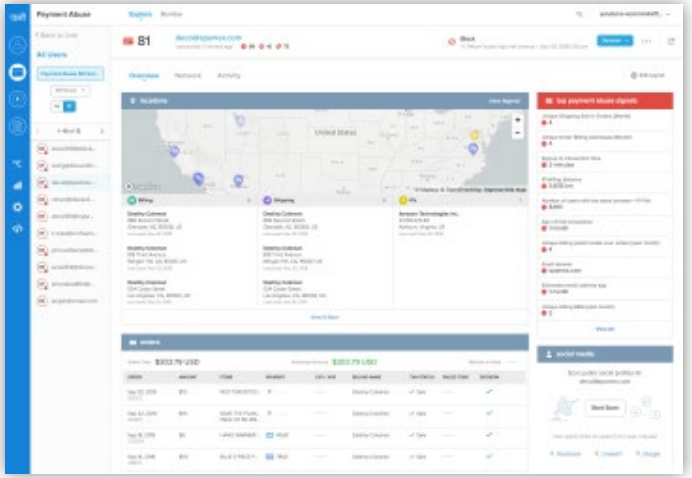
Account Defense

- Block fake accounts and risky sign-ups.
- Stop account takeover attempts and secure trusted user accounts.
- Reduce friction for trusted users.

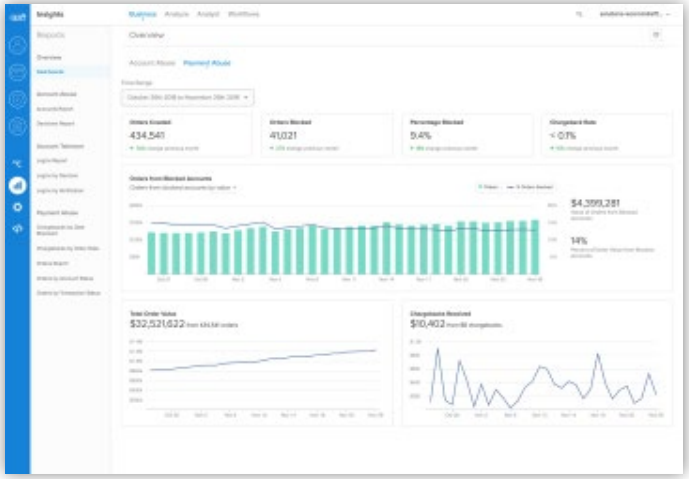
Content Integrity

- Reduce fraudulent content like spam and scams.
- Safeguard your brand and create better user experiences.
- Work efficiently and automate more reviews.

All of the above products utilize a single analyst console. The analyst console's 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** Score and expedite manual review decisions. This includes risky signals, locations of IPs, order and content history, and a network graph that shows all connected devices.
- **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. They also support escalation and hold functionalities for additional review by senior analysts or managers.
- **Automated workflows:** Analysts manage their business processes and decisions by defining automated workflows based on customizable criteria that can be layered using "if/then" analysis. Workflows are completely customizable and can be, for example, configured to automatically reject risky transactions, reduce friction for trusted transactions, assign transactions to fraud 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 their job needs. For example, admins may have access to manage workflows, analysts may have access to user details and make decisions, and a developer may only have access to integration health information. Customers can mix and match permissions to suit their team needs.
- **Multilevel account support:** Customers can set up sub-accounts within a global account to support multiple business units, geographic regions, etc. Sub-accounts are easy to jump between, and the global view provides comprehensive insights on all sub-accounts.
- **Real-time analytics:** Admins can track business health with comprehensive insights that report on order block and accept rates, chargeback rates, risky users, and more.
- **Built-in verification:** Customers can easily set up email or SMS notifications within the Workflows environment to authenticate any risky users who need an additional check.



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 & Safety Architects, all of whom are industry experts, are available for consultation to help teams of all sizes craft a holistic Digital Trust & Safety solution. 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 over the next 6-12 months:

- Robust multi-factor verification based on fraud risk
- Improved visibility into operational metrics
- Enhanced protection against account takeover and content-based spam and scam

Signifyd

Signifyd makes fearless commerce possible by providing an end-to-end Commerce Protection Platform. Powered by the **Signifyd** Commerce Network, the platform's advanced machine-learning engine protects merchants from fraud, consumer abuse and revenue loss caused by barriers and friction in the buying experience. A number of Fortune 1000 and Internet Retailer Top 500 companies are on **Signifyd's** client roster. They are headquartered in San Jose, CA., with locations in Denver, New York, Belfast, and London as well.

Signifyd helps merchants overcome key challenges by:

- **Reducing friction in the customer experience:** 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, a fast and secure checkout, real-time updates on order progress, and avoidance of step-up authentications become crucial.
- **Promoting revenue optimization:** At every stage of the revenue funnel, there are conversion drop-offs reducing the actual revenue realized from the original sales made online. To name a few, this includes pre-auth declines via payment providers, declines within the fraud management process, the lost revenue due to consumer abuse manifesting as returns, and chargebacks. **Signifyd** helps in analyzing these drop-offs. 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.
- **Enabling international expansion, cross-border sales, and PSD2 compliance in Europe:** Expanding ecommerce operations into new geographies is challenging. Fraud patterns, regulations, and the availability of data vary from country to country.

SIGNIFYD

At a Glance:

3rd Party API Capabilities

Machine Learning

Fraud Engine/ Platform Functionality

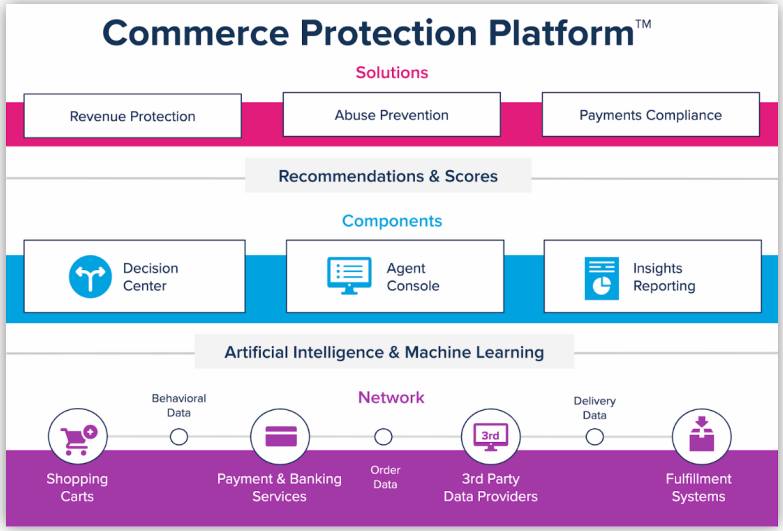
Account/Client Management

Guaranteed Chargeback Liability

Signifyd provides country-specific solutions including the capability to provide seamless SCA (strong customer authentication) via the 3D-Secure 2.2 protocol to comply with Europe's PSD2 requirements.

PLATFORM, SOLUTIONS & FUNCTIONALITY

Signifyd's Commerce Protection Platform is designed to provide the tools necessary for merchants to protect their shopping experience.



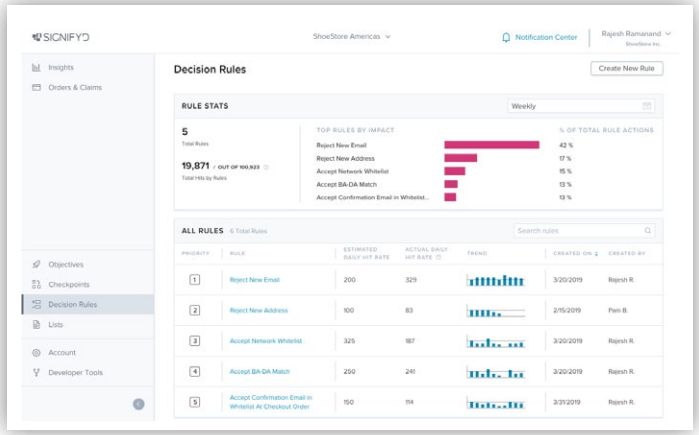
Signifyd's Commerce Network connects more than 10,000 merchants in all retail verticals and captures a diverse set of first-party transactional and behavioral data while leveraging integrations with third-party solutions across the ecommerce technology stack. The end result is an enhanced data profile for all types of transactions involving products shipped into 100+ countries across the globe. The network also incorporates data from multiple third-party providers, including a device identification vendor, email verification vendor, and several peripheral data vendors.

Signifyd's artificial intelligence and machine-learning engine is driven by a combination of both supervised and real-time machine-learning models, using random forest, logistic regression, and other techniques. The company runs multiple models in parallel and leverages their results depending on specific customer needs for distinct recommendations or to provide scores. Specialized models look at velocity, linking, aggregation, and other areas relevant to risk management

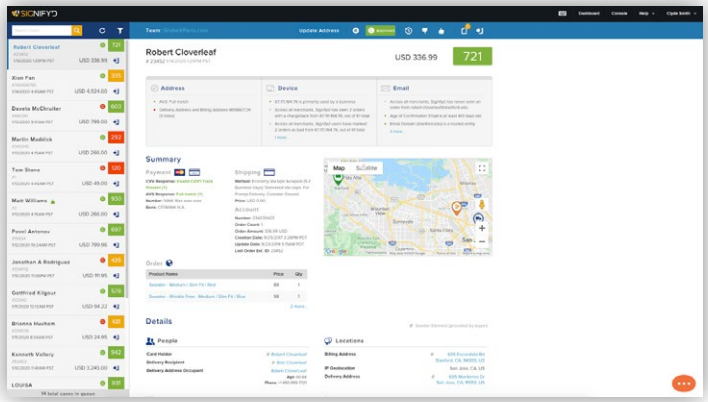
The three core components of the platform are **Decision Center** to automate business processes based on logic, **Agent Console** enabling employees to interact with specific orders, and **Insights Reporting** to provide the business intelligence necessary to optimize the overall shopping experience and revenue conversion.

Decision Center makes it possible for operations teams to automate business processes and enforce policies. For example, they can avoid promo abuse by directly leveraging a prediction of the expected outcomes. This allows merchants for example to address common business use cases such as auto-filling orders

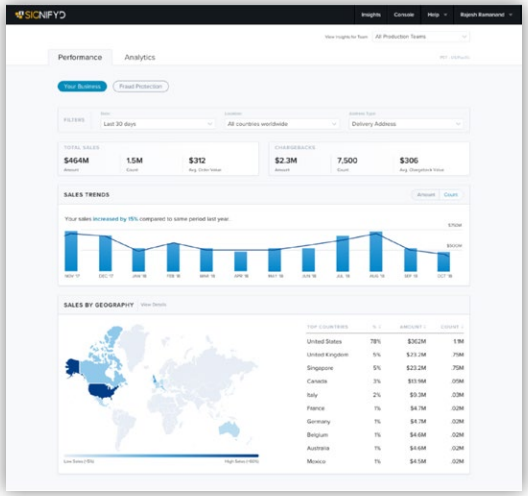
above a certain scoring threshold or orders that have been approved for a revenue protection guarantee. Through its API interface, **Decision Center** can leverage custom tools to further enrich data, initiate workflows through third party systems and trigger actions in third-party systems. **Decision Center**, in essence, becomes mission control to scale business while protecting the shopping experience.



Agent Console is an interface that gives agents visibility into specific transactions, including summaries, scores, recommendations, and the corresponding source data. **Agent Console** allows the end-user to interact with **Decision Center** and the underlying machine-learning model, for example, to escalate an order after augmenting some new information manually to reprocess scores or decisions.



Insights Reporting allows business users as well as data scientists to drill into the transactional data and derive insights on how their business performance varies between segments such as geographies, product lines, or payment methods. **Insights Reporting** comes with a fully functional user interface to visualize these insights and interact with the data dynamically



in real time. Merchants also have the option to connect the reporting data directly into their existing business intelligence systems via various integration options.

In addition to these core components, **Signifyd** also provides specific solutions that leverage scores or recommendations to fully eliminate the need for merchants to manage common use cases themselves:

Revenue Protection combines the underlying platform components with a 100 percent financial guarantee against chargeback losses on approved orders. This effectively shifts the liability for chargebacks away from ecommerce merchants. **Signifyd** charges a percentage of revenue and reimburses merchants for chargebacks resulting from transactions that its process approved. Merchants have the option to leverage this service for all their transactions or subsets such as specific geographies, product lines, or peak traffic during flash sales and the holiday season. Depending on the merchant needs, all chargeback types (including INR, SNAD, and others) can be covered by this solution.

Abuse Prevention combines the underlying platform components with active monitoring and investigations of consumer chargebacks as well as proactive consulting on best practices for business processes and policies, such as return policies. Chargeback data can be integrated directly via the payment gateways, and merchants have the option of letting **Signifyd** 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.

Payment Compliance 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 SDKs for mobile apps and ensures that the least amount of friction is leveraged dynamically for every applicable order.

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), Accertify, CyberSource, 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 6-12 months:

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

TransUnion

TransUnion believes that every consumer has a story. By uniting personal and digital identities via online and offline data, they can offer an accurate and precise data identity of a consumer, all while stewarding consumer data with care.

TransUnion offers the most comprehensive data identity platform inclusive of credit, public record, and reported history from devices. The breadth and depth of their data enables linkages and actionable insights through leveraging their historically strong modeling, data science, and machine-learning expertise.

With their **IDVision** with iovation platform, this intelligence can be applied by clients to quickly deploy strategies to secure trust, deliver friction-right consumer experiences while staying ahead of constantly evolving fraud tactics and complying with ever growing regulations. Verticals and industries of focus include: financial services, consumer lending, mortgage, retail/ecommerce, gaming, gambling, insurance, and government.

They maintain that fraud threats are prevalent throughout the customer lifecycle, growing in scope and complexity while user experience suffers. In addition, **TransUnion** recognizes that interactions through the mobile channel are increasing dramatically, surpassing desktop in many cases.

Solutions & Functionality

TransUnion's IDVision with iovation platform is a holistic fraud solution enabling businesses and consumers to secure trust and safely transact in a digital world. The **IDVision** with iovation platform, in conjunction with the recent acquisition of **iovation**, has created an enhanced level of functionality for their customers. While

At a Glance:

- Professional Guidance/Services
- Machine Learning
- ATO Detection Capabilities
- Account/Client Management
- Device Fingerprint Capabilities
- Fraud Engine/ Platform Functionality
- Historical Sandbox Testing

TransUnion

iovation's capabilities can currently be integrated as a stand-alone service (described on pages 34-38), the combination of the two platforms offers a complete solution to an organization's fraud challenges.

The full solution provides a multilayered approach that delivers a comprehensive picture of a consumer, allowing clients to establish identity, authenticate consumers, and prevent fraud. By offering a series of layer-able capabilities—each examining unique patterns of risk—customers can deploy strategies based on their organizational policies, regulatory environment, and levels of risk to fight evolving fraud tactics while securing trust with good consumers.

Establish Identity: By utilizing the service when an account is originated or provisioned, users can form a basis for greater identity confidence. This is achieved by verifying identity against a broad set of personal and digital identity data in order to optimize convenience and security while reducing occurrences of identity fraud. Examples of these identity elements include:

Identity Verification: Verify consumers using comprehensive historical data combined with predictive, cross-industry analytics. Merchants can access consumer records, government records and watch lists, suspicious and known fraud, blocked entities and persons, address change data, high-risk addresses, and phone numbers. They can gain insights into multi-industry behavior, suspect links and associations, synthetic fraud, utilization, and velocity. Assess risk scores with full context, including contributing factors, alerts, and match results.

FraudForce Device-Based Reputation: This utilizes powerful device recognition technology and a unique approach to device intelligence. It leverages device-to-device and device-to-account associations, device history, and 76M detailed reports of confirmed fraud from a global network of fraud and security analysts (iovation enhancement, described in full on pages 34-38)

Email address, phone number, and IP address verification: This provides an extra layer of risk insight at critical points including:

SMS one-time passcode: Before sending an SMS one-time passcode (OTP) to verify a user's identity, they assess the risk of the phone number.

Account origination: New emails are commonly used for synthetic identity fraud. So IDVision assesses the risk of submitted email and phone fields at account creation to distinguish the deceptive fraudsters from your good customers.

Account management: Account takeover attacks frequently attempt to change key contact fields. Check the phone or email details on an account before any account changes are made.

Checkout: Shipping fraud and payment fraud attacks commonly

use new email addresses and burner phone numbers. Evaluate the risk of the email or phone number at checkout, especially on guest purchases.

Phone number verification: This assigns a risk score to flag potential risk. The phone number risk score takes into account several indicators including previous fraudulent activity and other attributes such as carrier, SMS capability, and phone type. It also considers odd traffic patterns, as this may indicate that the phone is being shared.

Email Verification: This allows the riskiness of an email address to be assessed before deciding whether to accept it. They test the email address to uncover if it's valid and functional, how long it's been in use, how frequently it appears on sites across the network, and how popular it is on those sites. These details tell you a lot about whether you can trust an email address. For example, if the address is newly created and its level of activity is unusually great, you may choose to review or deny the transaction—particularly if you correlate the suspicious email activity with other device risk signals such as emulator usage.

IDVision Alerts: These leverage the power of TransUnion fraud capabilities by offering proactive real-time alerts via proprietary ID behavioral algorithms to pinpoint fraud and high-risk identities at originations, onboarding and throughout the customer lifecycle.

Verified Prefill: Organizations can increase conversions through simplified, safe application processing by reducing burdensome online forms to simple clicks by prefilling consumer PII through a triangulated approach that determines the identity of a consumer.

Authenticate Consumers: This layer verifies the consumer identity through risk-based authentication to enable meaningful experiences and offers that increase conversions and revenue. This is achieved by utilizing authentication at specific touchpoints while dynamically employing methods that match the risk level of the transaction. Examples of these authentication approaches include:

Knowledge-Based Authentication: This provides customers with thorough out-of-wallet exam sessions that vary in complexity depending on the risk of the transaction while providing compliance with Know-Your-Customer (KYC) regulations. Features include:

Extensive customization capabilities including variable length questions, complexity, data sources (credit and noncredit), and number of correct responses to meet your business requirements

Sophisticated logic in-exam creation with parameter driven questions, use of dummy or "red herring" questions, and configurable time to answer

Diverse, extensive data sources including demographic data, relative and associate data, credit data, property data and license data—

which reduces the likelihood fraudsters can obtain answers through public record searches or data breaches

SMS One-Time Passcode: Verify that applicants are associated with the phone number provided and issue a one-time SMS code to effortlessly authenticate identities.

ClearKey Device-Based Authentication: (iovation enhancement, described in full on pages 34-38) This provides a transparent second factor of authentication when combined with login credentials.

LaunchKey Multifactor Authentication: (iovation enhancement, described in full on pages 34-38) This multifactor authentication and authorization is delivered just-in-time tailored to risk level of transaction and business requirements.

Prevent Fraud: Through this layer, their customers are able to reduce risk and prevent fraud through risk assessment of transactions and identities by flagging suspicious behavior and inconsistent data for investigation. Examples of these capabilities include:

FraudForce Device-Based Reputation: This utilizes a powerful device-recognition technology and a unique approach to device intelligence that leverages device-to-device and device-to-account associations, device history, and 76M detailed reports of confirmed fraud from a global network of fraud and security analysts (iovation enhancement, described in full on pages 34-38)

SureScore Trust Indicator: This indicator predicts transaction outcomes based on device trust, transaction, and contextual or behavioral indicators. (iovation enhancement, described in full on pages 34-38)

Synthetic Fraud Model: This purpose-built FCRA-compliant model is designed to detect, remove, and monitor for the presence of suspected synthetic identities before lending decisions are made. The model boasts incredibly low false/positive rates, minimizing the potential impact to good customers while also mitigating the impact to key populations, including new-to-credit consumers, recent immigrants, and damaged credit

Fraud Prevention Exchange: This powerful industry collaborative is combined with **TransUnion's** entire network of available customer data. Gain a full industry view with flags for suspect ID elements and indications of suspect activity. Exchange members share select transaction data during the application process and certain outcomes from their verification activity. Indications of potentially fraudulent activity and reported fraud are carefully monitored to alert members when they are exposed to potentially fraudulent activity.

TransUnion

Fraud Models and Scores: Modeling and scoring includes industry-specific fraud models and rapid custom model development of bespoke models to address unique client requirements.

Investigations (TLOxp): These allow for simplified manual reviews to deliver additional information about people, businesses, vehicles, locations, assets, and much more. It can help organizations identify and map relationships for a more complete investigation and assist in proof-of-life investigations.

By offering a series of layered capabilities, each examining unique patterns of risk, customers can deploy strategies based on their organizational policies, regulatory environment, and levels of risk to fight evolving fraud tactics while securing trust with good consumers.

TransUnion offers a wide range of global coverage. Highlights include the following:

- **1 billion** worldwide consumer records
- **650 million** consumer credit history records
- **4.8 billion** monthly data updates
- **50+** petabytes of data
- **30+** countries

In conjunction with **iovation**, they can provide the following additional coverage elements:

- **6.5 billion** experiences with devices seen by network
- **45 billion** total transactions protected
- **26 million** transactions protected per day
- **76 million** fraud reports placed by network
- **35,000** websites and apps protected

Integrations and Services offered

TransUnion offers deployment of IDVision with iovation via simple API integrations. They offer flexible orchestration and integration options to meet customer business needs in any regulatory environment, including both PII-dependent or constrained environments. This includes both real-time or batch delivery, the ability to deploy the full suite of capabilities, or a select combination of capabilities.

Support and Training

TransUnion offers full customer support and training along with premium support options.

TransUnion

Included with all deployments:

- Post-implementation calibration services with a strategic fraud account manager, configuration monitoring, and bi-weekly reviews with customers
- Production support with systems impact monitoring, real-time alerts
- Solution training

Premium support options include the above plus:

- Dedicated customer success manager
- Weekly calibration reviews
- Value-added insights from **TransUnion's** research and insights analytics team tailored to a customer's business, use cases, and fraud or authentication concerns
- Weekly or daily product performance reviews
- Consulting services with operational calls, quarterly business reviews, and on-site support

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.

Brighterion

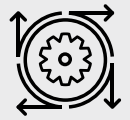
Brighterion is a fraud engine and platform which states they use more of an Artificial Intelligence (AI) approach to fraud prevention for merchants rather than traditional machine learning. They use one-to-one behavioral analysis to predict risk. They purport to use a single server to decision billions of events monthly. They further state they can decision "any data from any source at any volume."

They offer a few different products specific to merchants:

- **iPrevent:** A comprehensive approach to real-time omni-channel fraud scoring. They use their AI technology and other techniques to evaluate behaviors in real time.
- **iPredict:** Allows merchants to extract insights from their own data. The automation tools allow a merchant to evaluate the likelihood of specific outcomes.
- **iMonitor:** A monitoring solution that analyzes the performance of any analytical model. This tool purportedly reduces the need for manual rules creation by automatically generating decisioning rules.
- **iSupervise:** A graphical user interface (GUI) that provides non-technical access to end users to manage their queues.

Brighterion

At a Glance:



Machine Learning

Fraud Engine/ Platform Functionality

Brighterion 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

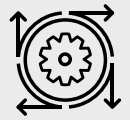
Feedzai attempts to provide a machine-learning-based fraud platform to help risk professionals do the work of data scientists using a guided, self-contained environment. Through **Feedzai DS**, teams are provided with a way to create advanced machine-learning fraud models. With extraction of features,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

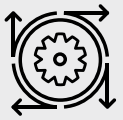
Feedzai chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

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:

Fraud Engine/ Platform Functionality

Guaranteed Chargeback Liability

Machine Learning

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.

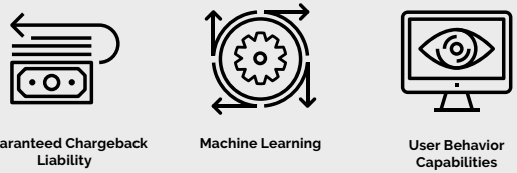
They offer a fully outsourced fraud solution, which includes a chargeback guarantee. While a full Application Programming Interface (API) integration is preferred, they do offer segmentation services like peak-season overflow volume and extreme high-risk products such as gift certificates. There's also 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.

Ravelin

Ravelin is a United Kingdom-based machine-learning fraud vendor that checks behavior against hundreds of fraud signals. Their system learns over time and gets more accurate as a merchant's fraud team makes decisions over time. **Ravelin** states that reducing chargebacks is their biggest priority. They provide a graph network analysis tool that detects connections between users in a merchant's customer base. They take a three-step approach to their product:

- **Integrate:** They use an application program interface (API) built to ingest relevant merchant data.
- **Interrogate:** Machine-learning models and a graph database analyze the data for good and bad behaviors.
- **Prevention:** On an ongoing basis, every customer action is scored for fraud probability, and **Ravelin** will tell users the impact to conversion.

Ravelin states that they're focused on reducing manual reviews to below one percent of all transactions, ensuring that the customer journey is positive and that decisions are automated and accurate. They say they have an API designed to ingest current and historical events from a merchant, including account creation, payment, checkout, and chargebacks. They state that they encrypt all of the data for maximum security and that their vault is PCI-compliant, allowing them to accept full card numbers.

Ravelin

At a Glance:

Machine Learning

Fraud Engine/
Platform Functionality

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

RISK IDENT

Risk Ident is backed by the Germany-based Otto group, one of the world's largest ecommerce companies. They rely on a heavy data science and machine-learning influence, with the goal to build a product that works now and can be updated later. This is achieved through a modern tech stack as well as a flexible in-house development and deployment approach. All technology is internally developed using additional data sources from a number of third-party providers.

Risk Ident utilizes three primary technologies to help merchants mitigate against fraudulent user attempts.

First, **Risk Ident's** device analysis and recognition solution is one of the very few device identification solutions that can provide a device ID under strict German privacy laws. Device Ident ensures that fraud correlations can be identified consistently. Access to push email and application programming interfaces allows individual assessment of device information in real time.

Risk Ident's second key technology, **FRIDA**, offers transaction linking and case management. **FRIDA** is a fraud platform and user interface allowing fraud agents to effectively manage and identify fraudulent transactions by combining a wide range of information sources.

FRIDA not only analyzes individual transactions, but it also compares previous account behavior, establishes relationships between transactions, and detects suspicious access patterns. Incoming transactions are automatically scored and connected, allowing fraud cases to be detected quickly. This helps **FRIDA** identify patterns and linkages that a human might overlook.

RISK IDENT

At a Glance:

3rd Party API Capabilities

Machine Learning

Risk Ident 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.

RISK IDENT

Through the user interface, fraud managers have an overview of potential fraudulent activity. In order to address the stringent data protection requirements under German privacy law, **FRIDA** can be used as a SaaS or may be installed directly on premises, enabling the customer to retain all user data inside the company, which is a benefit accorded to clients beyond Germany.

EVE, Risk Ident's third core technology, provides intelligent risk management based on past fraud agent decisions, overall data distribution, and feedback from confirmed fraud and non-fraud cases. Using **EVE**, the fraud agent not only sees a fraud score and an explanation of fraud indicators, but also the most probable type of fraud detected by the system (such as identity theft, account takeover, etc.).

In ecommerce environments, the **EVE** machine-learning technology is most commonly applied within the **FRIDA** platform. While the **FRIDA** platform historically utilized a rules-based approach, the **EVE** machine-learning engine supplies data-based decisions and scores calculated via machine-learning.

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

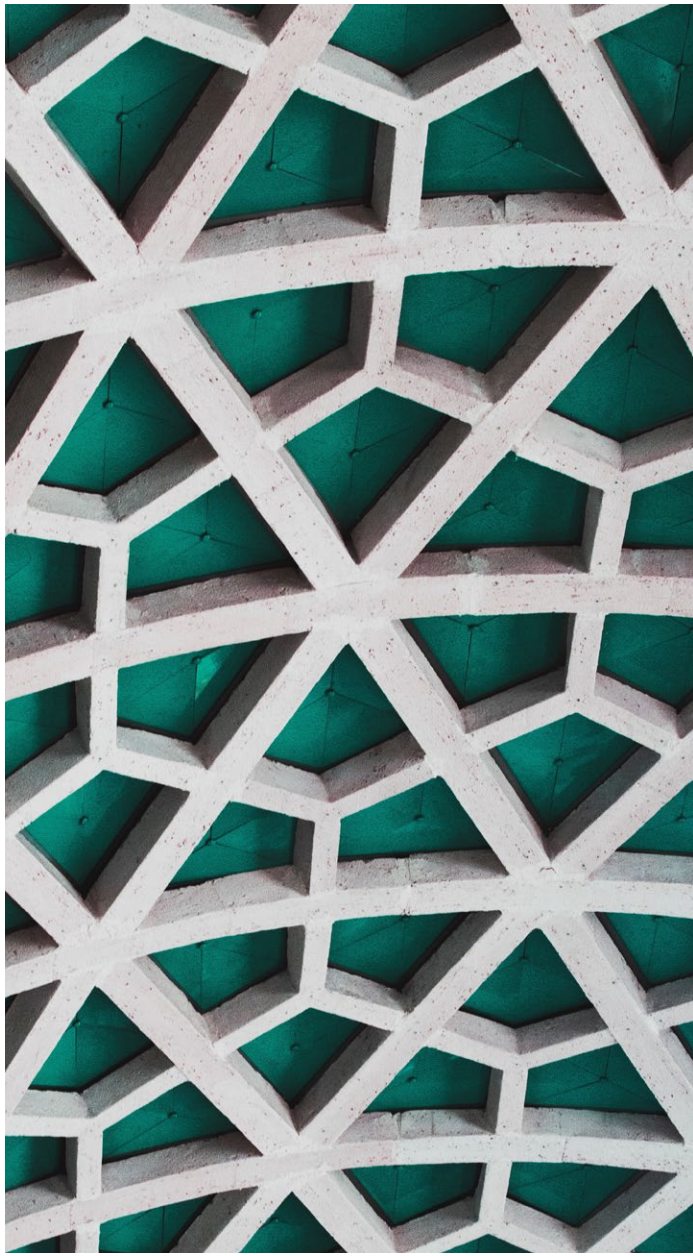
Fraud Engine/ Platform Functionality

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:

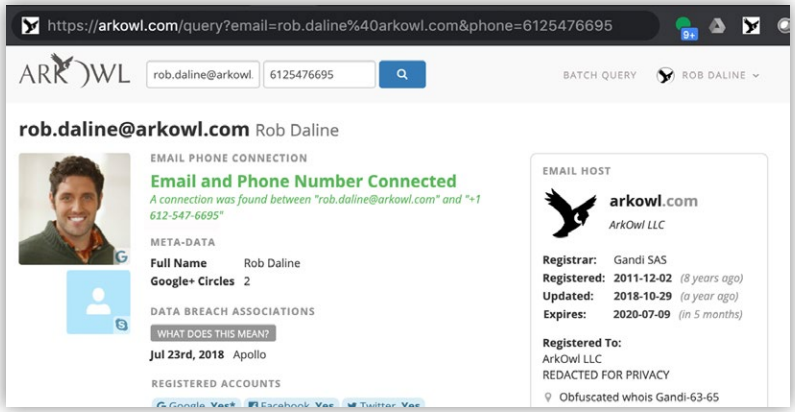
3rd Party API Capabilities

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

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 cross-border businesses grow revenue by maximizing their predictability of good transactions. Their product suite provides accurate identity data and insights to reduce fraud and mitigate risk for companies around the globe.

The **Ekata Identity Engine (EIE)** powers **Ekata's** identity verification solutions. It's the first and only cross-border identity verification engine of its kind. It uses complex machine-learning algorithms across the five core consumer attributes of email, phone, name (person or business), physical address, and IP to derive unique data links and features from billions of real-time transactions within the **Ekata** proprietary **Identity Network** and the data licensed from a broad spectrum of global providers within the Identity Graph.

The **Ekata Identity Engine** is comprised of 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** identifies behavioral patterns that pinpoint legitimate versus fraudulent behaviors behind online transactions. Leveraging **Ekata's Machine Learning Lifecycle Platform**, this real-time behavioral analysis measures and delivers transaction velocity, merchant popularity, and attribute volatility features.
- Since the launch of Confidence Score in 2016, **Ekata** has been committed to continually improving their **Machine Learning Lifecycle Platform**. Today, **Identity Network**, Confidence Score, and unique derived data attributes (like IP risk) provide

EKATA
LINKING DIGITAL IDENTITY BACK TO HUMANITY

At a Glance:

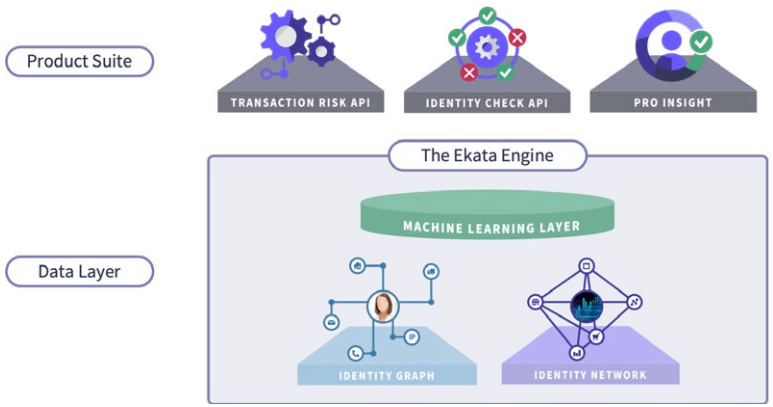
3rd Party API Capabilities

Machine Learning

Pre-Authorization Functionality

Account/Client Management

signals that help customers authorize good transactions, smooth new account opening, and catch more fraud. **Ekata's** proprietary testbed allows them to test the predictability of a new feature in as little as 15 minutes.



Businesses around the world utilize **Ekata's** product suite to increase approval of more good transactions, reduce customer friction at account opening, and find more fraud.

With over 20 years of data science experience, **Ekata** helps companies verify trusted identities while fighting fraud in industries such as ecommerce, online lending, payments, marketplaces. The details below focus on their flagship products, **Transaction Risk API**, **Identity Check API**, and **Pro Insight**, which can solve a variety of business problems, but are especially relevant in ecommerce segments like physical goods, and digital goods.

There is increasing traction for the **Ekata** solution in travel and hospitality, fintech, and online gaming as well.

Solutions and Functionality

Ekata's approach to fraud prevention finds a balance in approving more good transactions to keep customer insult rates low while reducing the risk of fraud. Their product suite includes APIs to leverage in automated rules-based decisioning platforms and machine-learning models, as well as a web-based SaaS tool to leverage for manual review.

Security & Privacy First

To **Ekata**, maintaining the privacy and security of personal data is paramount. To ensure the privacy of their customers and sensitive data, the **Ekata Identity Network** operates on highly obfuscated data. Comprised of thousands of participating customers, **Ekata's** proprietary Network provides the benefit of reducing privacy, regulatory, and security risks.

To ensure the privacy of customers and their sensitive data, **Ekata** operates on data that is hashed and encrypted using National Institute of Standards & Technology (NIST) recommended methodologies.

EKATA

Ekata prioritizes respecting the individual rights of data subjects. They provide identity verification and fraud prevention services worldwide, adhering to global standards such as the GDPR and CCPA to protect customers and their identities.

Transaction Risk API

Built specifically for models, **Transaction Risk API** provides predictive identity verification features (including Transaction Risk Score, Network Score, and IP risk) in a response time under 100 milliseconds. This maximizes predictability of good transactions, reduces false declines, minimizes customer friction, and reduces risk in real time. **Transaction Risk API** helps global businesses maximize performance by improving the efficiency of authorizations and reducing fraud rates. They score the overall risk of the identity behind a transaction, then deliver a response designed for easy model integration at scale.

Features:

- **Transaction Risk Score:** This is a real-time, predictive score derived from **Ekata's Identity Network** and the core identity data inputs of email, IP, phone, address, and name (personal/business).
- **Low Latency:** Ekata's cloud-based infrastructure delivers in under 100 milliseconds.
- **High Predictability:** The response includes predictive identity verification features to improve model performance.
- **Easy Integration:** The API response is feature-ready for ease of testing and integration into existing models.
- **Scalability:** Flexibility supports large throughput requirements, up to hundreds of queries per second.
- **Global Coverage:** Reliable data from around the globe offers broad coverage and accuracy.

Identity Check API

In a single query, the **Identity Check API** returns 70+ data signals and network insights (including **Confidence Score**). It provides validity flags, offers enriched metadata, matches statuses, and makes distance calculations between the key identity data elements of name (personal/business), email, phone, address and IP. The **Identity Check API** supports up to two sets of inputs (primary and secondary) for name, phone, address, and email, and one IP address. The sets of inputs include highly predictive information such as: email first seen, email match to name, phone match to name, IP distance from address, and a host of other inputs that can be hard to fabricate. This API was historically North America-centric, but has become increasingly global.

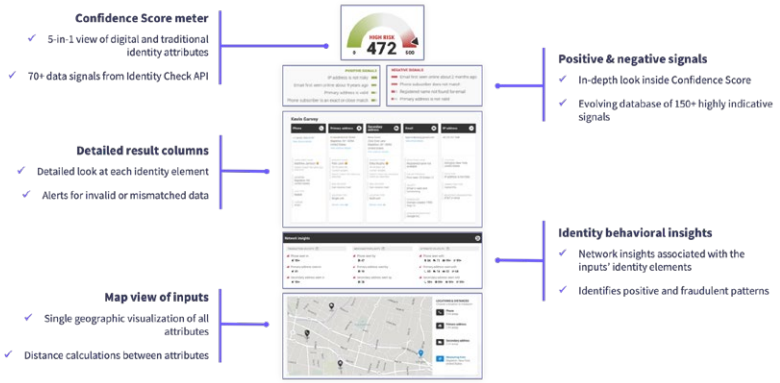
Features:

- **Confidence Score:** A real-time, predictive score that **Identity Check** derives from 70+ data signals and transactional patterns from **Ekata's** proprietary **Identity Network**, and machine learning.

- **Name Checks:** Verifies if the name matches the provided addresses, emails, and phones.
- **Phone Checks:** Shows whether the phone numbers are valid, their country codes, and if they match the names and addresses provided.
- **Email Checks:** Indicates if the emails are valid and active, surfaces first-seen dates, and shares whether the registered email names match the names provided.
- **Address Checks:** Specifies if the addresses are real, valid, and if the resident names match the names provided.
- **IP Address Checks:** Shows if the IP is risky, verifies its location, and determines if a person is found at the address (whether or not the name matches the name provided).

Pro Insight for Manual Review

Pro Insight is a global manual review solution that includes six ways to search, as well as analytics and administration tools, in a focused user experience. Although Pro Insight is a web interface that allows for further investigation into the identity behind a transaction, users already familiar with **Ekata** Identity Check API will recognize elements of Pro Insight.



Features:

- **Identity Review:** The flagship search provides a top-to-bottom result that starts with the **Confidence Score**, as well as positive and negative signals that reveal what is powering the score for a given transaction.
- **Global Confidence Score:** The risk score has been moved to the top of the page to reduce agent review time. The score gives a quick first view of the risk associated with an identity by leveraging real-time global data, millions of transactional patterns across **Ekata's Identity Network**, machine learning, and sophisticated data science.
- **Key positive and negative signals:** These dynamic signals, weighted by impact and listed in order of importance, reveal the story behind the **Confidence Score**.
- **Network Insights:** View velocity, popularity, and volatility of multiple identity elements based on transaction frequencies, linkage history, and behavioral patterns.
- **Distance calculation map:** This is an interactive visual representation of the distances between the inputs of phone, billing address, shipping address, and IP.

- **Deep Dive:** Access details from Identity Review or search for an individual data point to find additional information such as associated people, address history, alternate phone numbers, and more.
- **Reports and analytics:** This is generated to help admins manage Pro Insight and provide analytics on data such as usage, users, and coverage—available in graph view, list view, and for export.

Confidence Score

In 2017, **Ekata** launched **Confidence Score**, which utilizes the 70+ data signals in the **Identity Check API** response and the **Ekata** Identity Network to deliver a simple, easy-to-consume score on a scale of 0-500, with higher scores indicating greater risk.

Ekata has invested heavily in **Confidence Score** over recent years. The score simplifies the process of managing the multitude of data combinations and possible API responses to deliver an actionable, aggregate risk level of a transaction. The **Confidence Score** is built on a machine-learning model that calculates attribute values from **Ekata's** proprietary network, then feeds it into the scoring model along with 70+ data signals to calculate the overall **Confidence Score**. This drives more accurate and efficient decisions in both automation and manual review. Essentially, the score tells merchants in plain numerical terms how much it believes a transaction is good or bad. Strong correlations can help support accurate, confident decisions on both ends of the spectrum. Powered by a sophisticated engineering infrastructure, **Confidence Score** is calculated in fractions of a second and is available via the **Identity Check API** as well as **Pro Insight's** Identity Review. A low-latency version is included in **Transaction Risk**, displayed as Transaction Risk Score.

Integrations and Additional Services Offered

Beyond a standard set of customer management services, **Ekata** strives to ensure that its clients are effectively utilizing their services, whether they are using a direct API integration for modelling, improved rules-based decision-making, or **Pro Insight** for manual review. They offer a team of Solution Architects who work closely with clients to ensure proper testing, integrations, and ROI analysis—plus recommended rules, modelling, and best practices to get the most out of their services. **Ekata** also offers enterprise-level functionality including SSO, admin reporting, and 24-hour support.

Ekata offers developers the ability to access APIs through self-serve trials to best test and integrate for Proof Of Concept (POC). Once keys have been provisioned, developers can access a portal for testing other APIs.

EKATA

Ekata is a market-driven organization and takes customer feedback very seriously. The team makes an ongoing effort to understand their domestic and international markets, visit customers and prospects, and use that knowledge to drive the innovation of their products.

Pro Insight Integrations

- **Hyperlinks through existing partnerships:** Generally, merchants can activate a hyperlink in their existing fraud platform to access **Ekata Pro Insight** manual review solution with a single click. Existing partnerships include **Accertify**, **CyberSource**, **Experian**, and **Kount**.
- **Custom hyperlinks:** are also available for other case management systems to enable users to expedite identity review searches during manual review with a single click. These hyperlinks prvide a URL to directly populate transaction details (names, addresses, phone numbers, IP address, and email addresses) and access the **Pro Insight** results. Direct hyperlinks eliminate the need to use multiple vendors for single attributes. They also eliminate the need to copy and paste customer details into multiple search windows to verify an identity.
- **Ekata Hyperlink Builder:** Hyperlinks can also be accessed through a free Google Chrome browser extension that works with any browser-based case manager. The extension pulls elements from a transaction to populate an identity review result with a single click.

Identity Check API Integrations

- **Direct platform partnerships: Ekata Identity Check API** data can be activated on a platform to enhance an existing model and rule set. Through this process, clients can achieve a more cohesive and accurate prediction. Unique integration approaches are taken based on the specific platform. Merchants can activate the **Ekata Identity Check API** data through many existing partnerships, including **Accertify**, **CyberSource**, **Experian**, and **Kount**. The **Ekata** team or platform service provider can custom-tune these combinations of rules based on the customer's needs.
- **Direct integration: Ekata** provides extensive developer documentation for API integration. Documentation includes all possible values, request samples, and responses samples.

Identity Check API Integrations

- **Direct integration: Ekata** provides extensive developer documentation for API integration. Documentation includes all possible values, request samples, and responses samples.

EKATA

In Development Over the Next 6-12 Months

Global data expansion: The **Ekata** data science team takes a country-by-country approach in attempts to source the highest quality data available from reliable vendors, while continuously improving processing capabilities for countries of varying standards, laws, and regulations. **Ekata** is GDPR and CCPA compliant.

In 2019, **Ekata** added over 300 million records to the Identity Graph with significant increases in address coverage for France, UK, and Germany. They also added Brazil phone data and new email data links globally. These data updates grew the number of names in the Identity Graph that are linked to both digital (email, VoIP phone, IP) and traditional (address, landline, phone) data attributes across three continents.

Ekata will continue to focus on global expansion, with emphasis on expanding identity data coverage for email, address, and phone, adding over 100 million new links across western Europe and adding business data to the Identity Graph. **Ekata** is expanding identity data across Southeast Asia in 2020; these efforts will support the opening of their new office in Singapore early in 2020.

Product Improvements: Ekata continues to focus on developing and improving solutions based on customer feedback and market demands. In 2020, **Ekata** will be focused on two major product innovations. First, strategic data insights derived from the Identity Network and key predictive behavioral attributes will be added to more products in the portfolio to help customers identify fraudulent behaviors. Second, the roadmap includes exploring more account protection offerings, working to eliminate friction while supporting the good, profitable business.

Infrastructure Improvements: Ekata plans to continue infrastructure improvements into 2020. These improvements will provide customers with higher speed, reliability, scalability, and security. By utilizing cloud computing and advanced engineering, they can constantly monitor, measure, and refine their data in order to deliver identity data in sub-second response times to businesses globally.

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

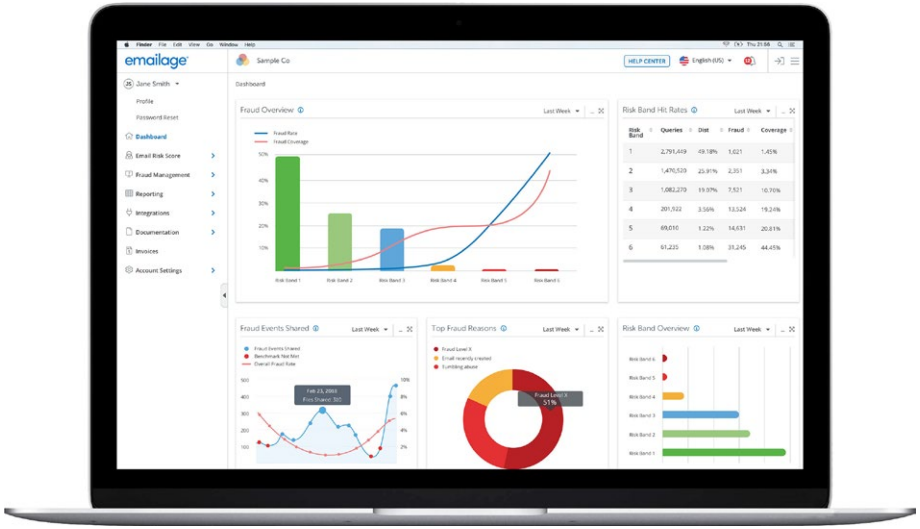
Emailage

- 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.

Emailage

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.

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.

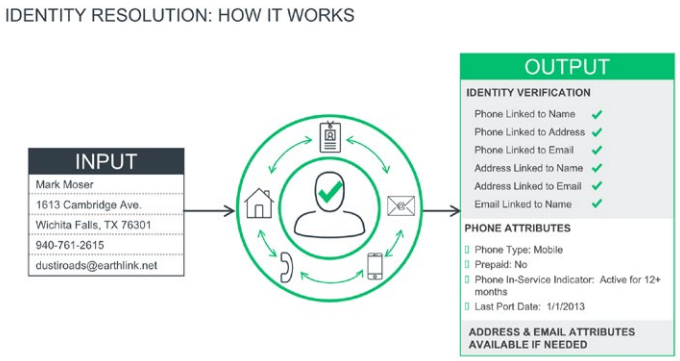
Neustar

Neustar helps businesses identify fraud risks and increase consumer trust by having a clear understanding of the person behind every transaction or interaction. **Neustar** fraud solutions provide the "unstealable" consumer insights needed to know with certainty who is at the end of every interaction, creating trusted and frictionless consumer interactions.

Leveraging an authoritative network of physical, digital, and device identity data, in addition to other signals like browsing footprint, **Neustar** allows merchants 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, operational efficiency (IVR/contact center), right-party contact rates, revenue-per-dial, average call handle time, lifetime customer retention, and customer satisfaction.

Solutions & Functionality

To **Neustar**, "identity resolution" means using a host of authoritative identity signals to quickly identify, authenticate, and fast-track legitimate customers and transactions while mitigating against as much negative impact of fraud as possible. The more accurately consumers can be identified, the harder it is for malicious users to spoof identities. It



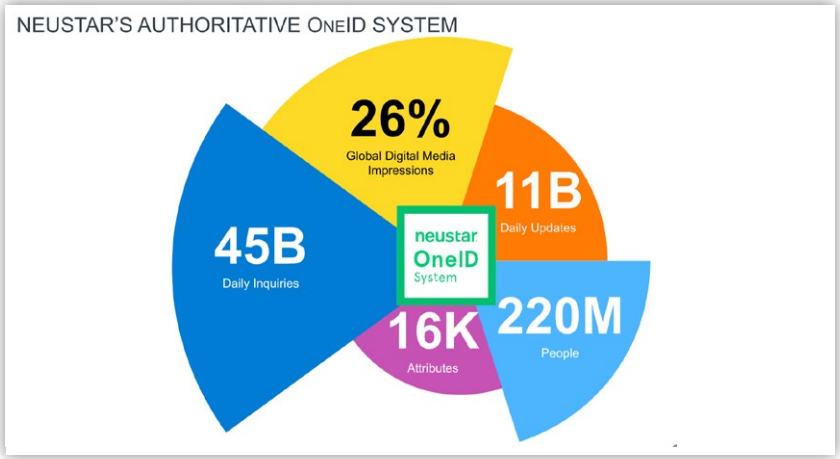
neustar®

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

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.

This is achieved through the **Neustar OneID** system—a repository of online and offline data that is broken down, corroborated, and rebuilt every 15 minutes with updates from sources with direct billing relationships. **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. 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 is focusing additional resources in 2019 to develop a phone reputation score that helps users identify potential of such an attack.

These technologies can be applied in a number of ways, for a number of organizations, across vertical and industry. They allow **Neustar** to help users focus on mitigating reputational harm, financial impact, and negative customer experience.

There are four primary product offerings:

Digital Fraud

- **Digital Identity Risk** uses a wide range of device-based intelligence to separate legitimate users from fraudsters. Using a number of digital elements, including IP, browsing, phone activity, and connections to digital footprints to person

or household, **Neustar** corroborates the digital information against offline consumer data and provides 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.

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:

a. **Pro Level** combines a wide range of intelligence about users, including device, IP history and characteristics over time, advertising and publishing key signals, what websites this device has visited, and indicators of potential threats.
b. **Flex Level** extends the reach of clients with fewer integration and data science resources. It utilizes fewer signals, which are more easily consumed while allowing users add data elements over time.
c. 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

- **Outbound Risk** helps organizations ensure that their outbound messages reach the intended consumer. 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, and the result is that fraudsters may intercept two-factor authentication calls or texts to commit account takeover fraud. Using **Outbound Risk**, **Neustar** can help identify phone numbers at high risk for fraud. They do so by addressing the three attack vectors below.
  - **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** uses a simple API call. Users can 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. Continuous monitoring is commonly used where financial, reputational, and regulatory risk are high.

- **Inbound Authentication:** This solution, which leverages **TRUSTID** Authenticator 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. Inbound call agents are presented with a "green" or "red" authentication token, which can be used to manually or automatically route the call to the appropriate agent, or contain it within the IVR. If the caller cannot be identified by their phone number because of a lack of match with the CRM record, **Neustar** uses authoritative data to link the number to the correct consumer household in the CRM database. Integration with a user's decision engine can allow the combination of products for a customized approach.

Since the acquisition of **TRUSTID** in 2018, **Neustar** has incorporated **TRUSTID's** authentication solutions to its inbound call products and solutions. **TRUSTID** works with financial institutions and other organizations to authenticate callers, protect account access, and prevent fraud or comply with regulations. Since the acquisition, **Neustar** has invested in progressing their ability even further to provide authoritative call center intelligence. This progression has come through multiple initiatives:

- Utilizing **TRUSTID's** call path forensics in conjunction with **Neustar's** deep insight into ID verification. This lets users know that not only can they trust the call but they can trust that the caller is the customer. This increases their ability to identify legitimate customers up to 70%, which helps reduce friction and fast-track users. The remaining 30% can receive the normal level of friction or be routed to specialized teams.
- As early adopters of the emerging "stir/shaken" technology, **Neustar** provides the ability for carrier-based authentication of actual phone users. Also, **Neustar's** proprietary attestation certification could allow for a longer-term increase in authentication of call sources (robocalls, etc.).

- Finally, **Neustar** has improved ability to identify sim swap and call-forwarding requests (including "recency" of request). This helps mitigate against malicious password reset and OTP requests, avoiding these potentially high-risk scenarios. By using this level of detail to route calls to agents trained to handle these scenarios, or contain them entirely within the IVR, clients can better optimize handle times and costs.

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

TRUSTID Acquisition

In late 2018, **Neustar** acquired **TRUSTID**. With the acquisition, **Neustar** has incorporated **TRUSTID's** authentication solutions to its inbound call products and solutions. **TRUSTID** works with financial institutions and other organizations to authenticate callers, protect account access, and prevent fraud or comply with regulations.

The complementary services were already bundled together through a partnership, but the acquisition helps move the technology further up the technological hierarchy and allows for more sophisticated forensics by utilizing a more complete suite of tools. Enterprises will more quickly and accurately have access to data designed to help them know who is on the other end of the phone. It both increases efficiency and further optimizes costs.

Services offered:

- **Neustar's** client success teams include project management support. In some cases, clients will 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.
- In addition to recent device ID developments, **Neustar** is investing in identity velocity features in the near future. These will use the amplitude of access and changes to a specific identity to contextualize use of that identity across **Neustar's** portfolio.

PIPL

Pipl is a leading provider of trusted global identity information. Their products and services are used by top ecommerce businesses, insurance and financial institutions, media companies, and governments around the world to reduce investigation times and provide frictionless customer experiences.

Pipl's proprietary identity resolution engine cross-references public data from the internet, listings, directories, archives, and exclusive sources to produce a data index. It has widespread global coverage including emails, mobile phones, social media profiles, associations, and more.

At a Glance:

3rd Party API Capabilities

Pre-Authorization Functionality

Solutions & Functionality

Primary solution offerings fit into two distinct categories:

- **Pipl SEARCH for Manual Review: 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 various locations, emails, people and businesses. Conversely, it can tell you if the buyer is likely to be using false or synthetic identity information. This increases the opportunity for a team to approve or deny global transactions in a more expedited way.
  Key Performance Indicators (KPIs) of focus through the manual review solution include: Case Time/Operational Cost, Case Resolution rate, and Verification Accuracy.
- **Pipl API for Automated Identity Verification:** The **Pipl** Data API helps companies automatically verify identities across their decision platforms. These global organizations know that the breadth and depth of **Pipl's** public identity information lowers risk, lifts approval rates and reduces revenue losses due to fraud and chargebacks—all while providing a friendly frictionless customer experience.

Key Performance Indicators (KPIs) of focus through the manual review solution include: Verification Throughput, Verification Accuracy, Improved Bottom Line.

To ensure a good merchant fit, an extensive Proof Of Concept (POC) process exists for both search and API options.

- **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 which is provided at no cost to the customer after speaking to their dedicated account manager.
- **API:** A dedicated customer success engineer performs a data evaluation plan with the customer at no charge to ensure success. "What if" Analysis is available by utilizing either a test file (xls, csv, etc…) or by integrating the API into their test environment, customers can use the timestamps in **Pipl's** data response to establish value using their historical data set.

Reporting

Pipl customers are assigned dedicated account management resources to help customize the reporting of SEARCH and API 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 API 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:** A monthly license fee applies per user, with unlimited searches
- API: Transaction-based
- Custom pricing and packaging options are also available

Integration options

Integrations options into **Pipl's** API can be found at https://docs.pipl.com. 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 in 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

A Customer Success Engineer and Data Integration Expert will be assigned to all customers at no additional cost and will provide ongoing and continued support.

In the coming months:

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

- Continuous expansion and refinement of their massive data index
- Investigation features
- Verification features
- Data as a service (DaaS) performance

Socure

Socure's approach to identity verification and fraud prediction is predicated on the notion that consumers today lead very digital lives, leaving breadcrumbs naturally about themselves both online and offline. For the digital world, **Socure** provides a real-time predictive analytics platform that combines the newest forms of machine learning and artificial intelligence with digital and offline data. This allows them to deliver the most accurate and robust Know Your Customer (KYC) identity verification and fraud risk prediction solution in the US market—at the Day Zero stage.

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

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

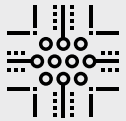
Socure uses multiple types of data sources, including traditional and offline data, real-time data, and social data to generate over 3,000 predictive variables associated with email, phone, address, DOB, SSN, device, IP, name, and physical documents, among others. The internal and third-party data sources 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 and proprietary alert list databases in developing its machine-learning models.

At a Glance:

Machine Learning

Device Fingerprint Capabilities

Pre-Authorization Functionality



Non-Production Real Time Rules Testing

Socure

Socure's fraud and identity solutions were designed and optimized to primarily focus on the riskiest top two to three percent of applicants, drastically increasing fraud capture and reducing FPRs in the smallest review and decline populations possible. Through this focus on accuracy, they support a number of use cases, both pre- and post-authorization—such as new account creation, sign in, guest checkout, account changes, etc. The company serves a wide market base where identity verification is particularly valuable, such as financial services, ecommerce, shared marketplaces, telecom, healthcare, insurance, and the federal government.

Solutions & Functionality

Socure Sigma Fraud Scores provide industry-specific machine-learning models that have been trained with their top 150 fraud predictors, using both good and fraud performance feedback from a consortium of the company's top clients in the major industry sectors. **Sigma Fraud Scores** are 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 Scores** are designed to capture multiple identity fraud types, typically decreasing new account fraud by >80 percent in just the top two percent of risk at better than 1:1 false positive rate. Many customers have also seen manual review rates cut by >75 percent and the number of approved accounts and transactions increase by >10 percent.

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. **Risk Scores** identify more than 40 percent of all fraud and 98 percent of all fake emails, phone numbers, and addresses.

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 >96 percent 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 Field Verification: Traditional Know Your Customer (KYC) solutions that rely on credit data tend to reject (or subject to huge amounts of friction) a large quantity of legitimate young, immigrant, and thin-file individuals who commonly have low credit usage and/or frequently change their home address. The **Socure KYC/CIP Field Verification** compliance module verifies first name, last name, address, phone, DOB, and SSN correlation in order to build a passive Customer Identification Program (CIP) that doesn't interfere with the account opening experience.Through this streamlined KYC solution,

clients can expect an expedited new account opening process, allowing clients to significantly increase auto-accept rates by 30-60 percent to >90 percent while substantially reducing friction for legitimate users.

Document Verification is available via the API and Mobile/Web SDK to provide accurate secondary identity verification while also reducing the friction associated with legacy Knowledge-Based Authentication (KBA) approaches. **Socure Document Verification** ensures that the document presented is authentic, and it then uniquely correlates the Personally Identifiable (PII) elements presented in the application (Name/Address/DOB/Selfie) to those OCR'd from the document. 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, Mobile or Web SDK.

Anti-Money Laundering (AML) Watchlists: Socure's AML Watchlist & Sanctions Screening is designed to minimize false positives with the flexibility to make separate watchlist calls, as companies performing an AML watchlist lookup are mandated by law to investigate any match that is returned from their solution provider.

Alert List: A consortium database of over 150 million records of first- and third-party fraudulent identities, tagged per industry, leverages **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) in its service. This proprietary and mostly-automated approach serves to develop highly predictive positive or negative correlated features that are then used in subsequent re-training of their machine learning models. This continued learning, driven by performance feedback across all of its customers, serves as **Socure's** end-to-end machine-learning platform for building, training, and deploying highly accurate models. **Socure's** machine-learning models are continuously challenged with updated models to see if they can outperform themselves. This continuous loop is what produces the most up-to-date and relevant fraud, correlation, and risk scores possible.

Unlike some consortium services, **Socure** does not simply dump positive and negative feedback elements into a database. They take the next step by running statistical tests on feedback, using it to fuel predictive models. They believe that the real value of feedback is in how it is used to test data sources, develop highly predictive features and re-train its machine learning models.

International footprint: the product and services described above are currently focused on the U.S. market only.

Socure

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 meant to be actionable and highly accurate in solving specific problems. By plugging these answers into a rules engine, **Socure** is typically the first and most accurate decision point with its clients.

In the case of more sophisticated organizations, the responses can be "matrixed" or overlaid on top of their own existing ML models. This allows the user 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 is a lot of customer variability across different markets and client sizes, there are also a number of integration options for deployment. Beyond the API integration, 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 the 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 triangulation of 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 preset monthly minimums, a setup fee, and an annual license fee.

Flashpoint

Flashpoint offers data and analysis by looking at information in the Deep and Dark Webs. They help combat fraud stemming from detection difficulties, language barriers, technical complexities, and lack of visibility into the Deep and Dark Webs.

Their approach uses multi-lingual analysts immersed in the Deep and Dark Webs who analyze fraud across various illicit communities that use complex techniques, tactics, and procedures to engage in fraud. They combine analytical experience with counter-tactics and intelligence to help organizations proactively mitigate complicated fraud schemes.

They can use this information and analysis to determine if the fraud is ultimately the result of external fraud attack or one stemming from inside information being stolen and sold on the Dark Web by an employee or a contractor of a merchant. They purport to have a customizable dashboard for merchants to monitor threat vulnerabilities. This allows merchants to potentially see a deeper contextual analysis of what is transpiring on the Deep and Dark Webs.

FLASHPOINT

At a Glance:

3rd Party API Capabilities

Account/Client Management

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.

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.

LexisNexis Risk Solutions

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

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

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

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

LexisNexis® RISK SOLUTIONS

At a Glance:

3rd Party API Capabilities

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

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.

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.

Pindrop Protect

Pindrop Protect provides a risk score and call intelligence to call centers as a call connects. The risk score—along with the analysis of the caller's voice, device, and behavior—is provided to the call center's fraud analyst team for further investigation. **Pindrop's** proprietary machine-learning algorithms then use feedback from the investigation to maximize solution performance.

Fraud Detection: Pindrop Protect provides real-time risk alerts and call intelligence. For every inbound call, phoneprints and voiceprints are compared to known fraudsters, along with behavior anomalies that indicate fraud. **Pindrop Protect** provides alerts against reconnaissance tactics and robotic dialing techniques, preventing fraud before a transaction can occur. Analysis of flagged fraud calls provides feedback for advanced machine-learning models, allowing improved fraud detection capabilities over time.

Protect Results: Protect analyzes each call for fraud in real time and reduces fraud exposure and monetary losses that can reach well into the millions of dollars. Knowing the risk of each call relieves call center agents of the need to become experts in the latest fraud tactics. This can reduce or eliminate knowledge-based authentication questions, and allow agents to focus on providing better customer service.

Root Cause Analysis: Pindrop Protect's intuitive case management tool flags calls based on a customizable risk threshold. It then provides full audio playback along with the call's risk assessment, and enables fraud analyst teams to connect fraudsters working across multiple channels and accounts.

pindrop®

At a Glance:

3rd Party API Capabilities

Machine Learning

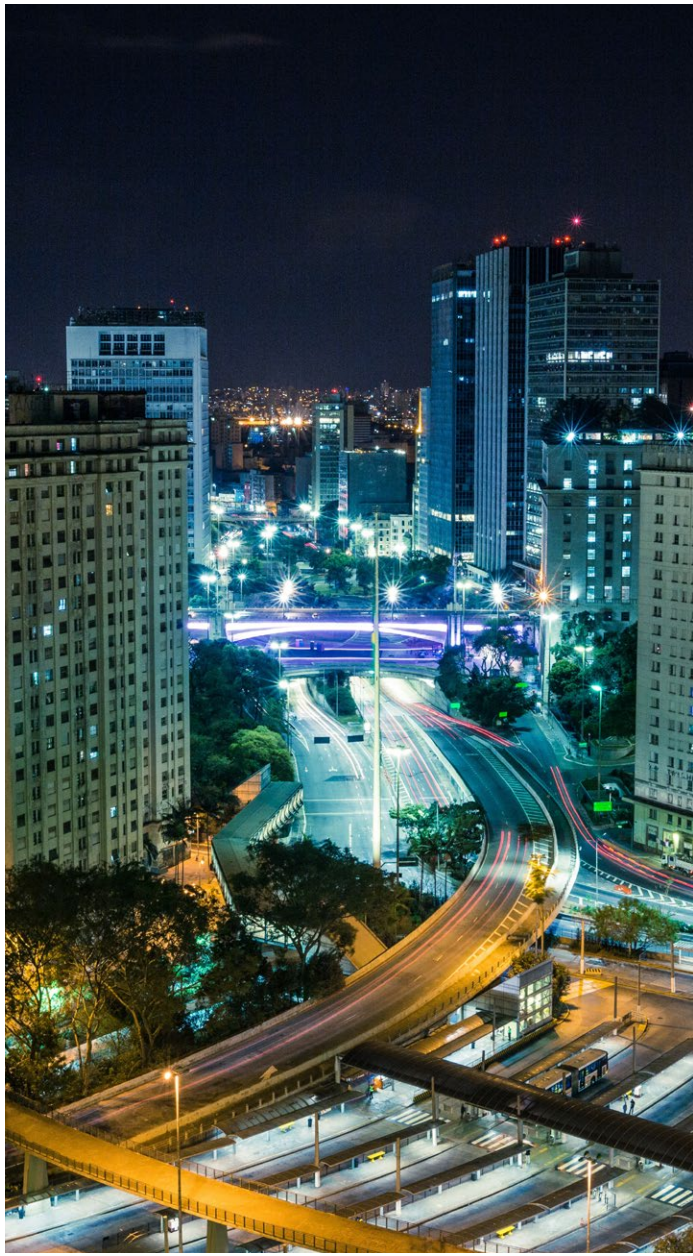
Pindrop Protect chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

Pindrop Protect

Passport Solution Experience: Pindrop Protect's authentication technology is based on credentials and risk criteria extracted from a call. These decisions are automated and governed through a flexible policy engine to build trust for genuine callers. Passport also provides critical insight into authentication performance, as well as key actionable intelligence about how callers are interacting with the IVR and agent.

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 is a leading provider of fraud prevention, chargeback management, digital identity, and payment gateway solutions to customers spanning ecommerce, financial services, and a diverse number of 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—without impacting the customer experience.

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.

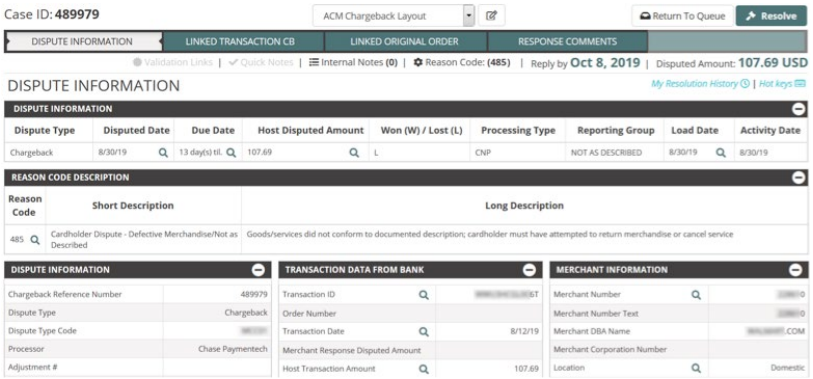


figure 1: user interface

Accertify
AN AMERICAN EXPRESS COMPANY

At a Glance:

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

Accertify Chargeback Services

Accertify's Chargeback Management solution can reduce the resources required to manage and respond to chargebacks by up to 50 percent. It offers a software-as-a-service platform that clients can manage themselves—or clients can outsource the end-to-end management of chargebacks using **Accertify's** Managed Services offering.

The platform offers the following:

- **Automated Processor Integration: Accertify** is integrated directly with most processors. Therefore, most chargeback files can be automatically and systematically imported into the platform without human intervention. In addition, chargeback responses can be automatically exported to integrated processors using similar technology.
- **Workflow Management:** The platform has out-of-the-box workflows and has the ability to create client-specific workflows based upon dollar values, chargeback reason, response date, and other similar data points.
  The automated document capture process offered by **Accertify** eliminates the manual processes traditionally required for uploading screenshots and printed documentation. This includes upload, copy/paste, and a repository for supporting documentation and compelling evidence for representment. 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 automated or semi-automated responses to the processors. This no-touch model works especially well for high-volume, small-dollar chargebacks.
- **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 that display trends for recently worked items while also providing a snapshot of what chargebacks are nearing their reply-by dates. This provides a clear understanding of whether the client's staff is keeping up with inventory.

  For simple reporting, 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 performance is reflected in won/loss success ratios in total dollar, case count, and percentage amounts for cases manually reviewed complete versus accepted. The platform not only provides insight into who last interacted with a chargeback, but it can also show an agent's average work duration for a specified period. Won/loss ratios can also be aggregated and grouped 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 the Fraud Platform. Information is automatically populated into the Chargeback Management solution and vice versa. Fraud and chargebacks form a symbiotic relationship, enabling each to seamlessly leverage and benefit from each other. This ensures they stay synchronized and realize their maximum potential.

  Accertify also partners with Ethoca and American Express and receives chargeback alerts in near real-time. This allows clients to react to change faster. They can potentially stop shipments and issue refunds—and improve prevention rules, strategies, and model performance while providing a better customer experience.

Chargeback

Chargeback is a Salt Lake City-based company established in 2011. Unlike most dispute management solution providers specializing in managed services, **Chargeback** provides software tools to help streamline the process of dispute management. This allows merchants to keep the process in-house.

Much of this focus is driven by the increased need to provide real-time dispute responses to issuers and networks. **Chargeback** believes that the Visa Claims Resolution (VCR) and MasterCom Dispute Resolution initiatives will drive this need even further.

Solutions & Functionality

For ecommerce and omnichannel merchants, dispute management can be a difficult process. Dealing with numerous unlinked sources of data can limit merchants' access to the evidence and the data points they need to make a decision. Deciding whether or not to respond to a dispute, determining what evidence to provide, and then compiling that evidence can be time-consuming and cumbersome. This can potentially erode the ROI of the process overall.

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 **Chargeback App** assists merchants in quickly taking actions like canceling an order and issuing a refund, or crafting a detailed document in support of a representment. The application provides guidance and support at each stage of the dispute lifecycle to ensure maximum recovery of lost revenue.

At a Glance:

Chargeback

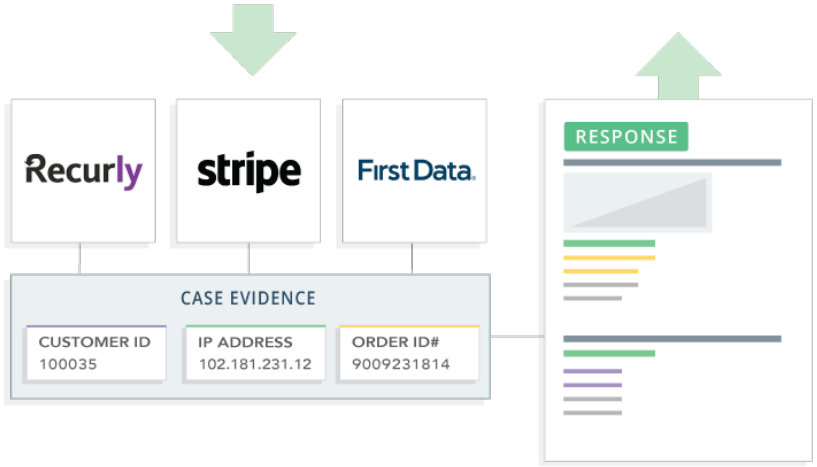
Most of the established providers in this market segment use a managed services outsourcing approach. Since access to the dispute data is commonly gained through a gateway or processor login, this can cause problems for many merchants not willing to grant the access due to security concerns. To address this issue, **Chargeback** has built a web application that retrieves data from the various systems and aggregates it into a single interface to build a response. Their focus is on giving access to all data their merchant clients need without requiring clients give up control of their systems, either internally or externally. The application pulls that information together with technology, not user access, and provides an interface that allows merchants to manage disputes and create responses.

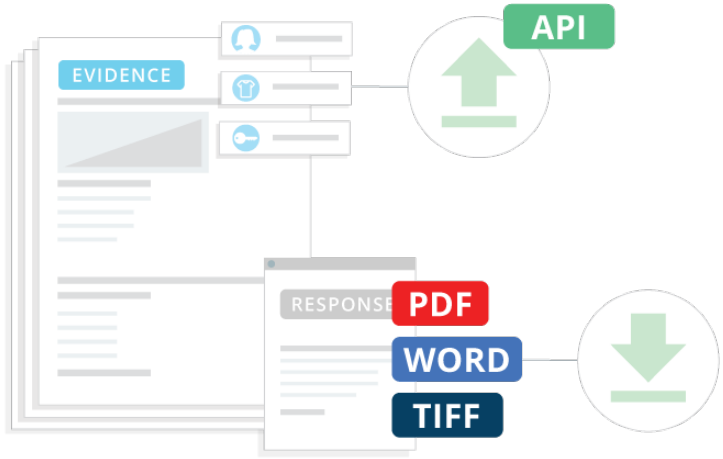
Built into the **Chargeback** app is an "expert system" knowledge base containing information on rules and regulations, submission guidelines, and more. This reduces the reliance that many firms have on their most experienced staff, who could potentially move on and take that knowledge with them. At the same time, **Chargeback** recognizes that there is a higher level of understanding and ability within the ranks of any merchant's own staff, compared to that of an outsourced chargeback response team. As such, the app provides the technology, which, combined with the inherent internal merchant knowledge, creates an effective combination.

Within the interface, users are provided a queue that allows visualization of all disputes at every stage in the chargeback process. Users can filter and assign by agent, add notes, and update labels. For merchants operating multiple sites or catalogs, a drop-down provides the ability to filter based on these subsets. Within transactions, users can view and apply evidence. The system provides the flexibility to handle evidence types from multiple verticals and industries. For example, in the case of physical delivery or pick up, users can apply driver's license scans, customer service documentation, and carrier tracking details. In the case of digital delivery, users can track subscription access, term and condition agreements, gift certificate usage, etc.

The **DocGen** automation in the **Chargeback** app provides a response generator, which can collect order, customer, transaction, and dispute data and add it to auto-populated responses. The responses address 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 attempt to ensure that optimal and applicable evidence is submitted. If there are certain types of evidence that are always applied in the same way, these can be automatically uploaded every time without additional user interaction.

Chargeback



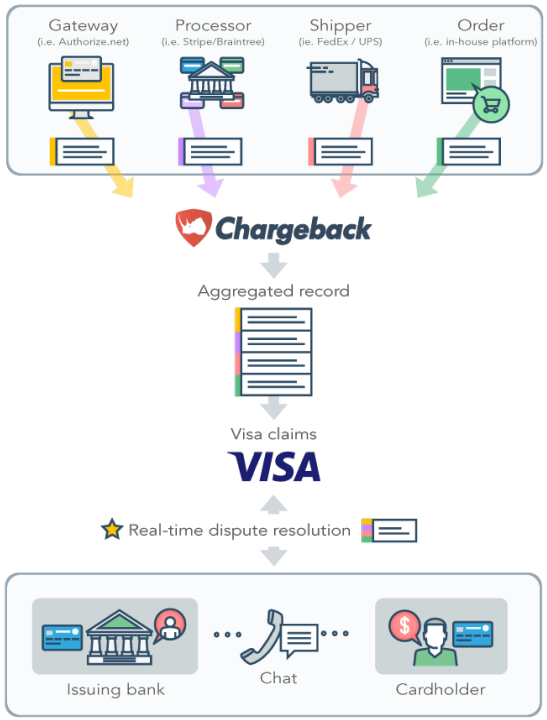


The technology can also review the geolocation details and provide any relevant supporting documentation in the event that these details fall within a narrow radius, often a potential indication of friendly fraud. The system can also automatically look up tracking details and add notes in the event of delivery and signature. One important note is that evidence is never applied that could potentially undermine the case.

Once complete, the support documents are created and submitted automatically using another automation tool inside the app called **DocSend**. It auto-sends completed responses in PDF or Word formats by email, fax, or upload, depending on requirements.

Through the application, merchants benefit from another automation tool: **Real-time Resolution**. This functionality allows merchants to provide customer, order, and product detail to Visa's dispute management platform—Visa Resolve Online (VROL). This supplemental information is combined with the related Visa 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 a better decision on whether to let the cardholder file a dispute claim—and if so, more accurately choose what type of dispute should be filed. Typically, this level of customer, order, 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.

Merchants can also receive **Alerts** in the **Chargeback** App, which are enhanced notifications that allow users to take actions to minimize losses and prevent chargebacks in the first place. These enable the merchant to initiate time-sensitive actions such as



stopping fulfillment, deactivating gift cards, cancelling 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, **Chargeback** offers a number of flexible options. The overview page offers a quick report of the "lay of the land," including overall volume, new alerts, dispute volume, and dispute outcomes. Timeframes include daily, weekly, monthly, and tracking over time.

Currently, the focus has been based on trying to give customers access to as much raw data as possible. This allows merchants to filter particular attributes. Feedback can then be applied to a number of data visualization tools.

Integrations

The **Chargeback App** can be connected through a number of existing integrations with many popular platforms including processors, gateways, and ecommerce shopping carts. Examples include Shopify, Cybersource, Magento, Vantiv, and WorldPay (among others). Specific merchant setup can vary based on platform. However, the list of integration partners is extensive enough to ensure a relatively seamless integration in most cases. The connections already exist on the provider's end, so merchants do not bear as much burden as they go live.

For merchants using technology not already integrated, **Chargeback** will work with the provider to create a connection. These connections are prioritized based on client demand and can influence the timeframe to integrate. **Chargeback** also provides

an "Orders API" for merchants with custom-built shopping cart platforms. **Chargeback** can also consume webhooks and connect to existing data warehouses.

In development in the next 6-12 months:

- **Ongoing expansion of supported data sources:** The expansion includes refund and credit history, customer history, previous stages of same dispute, and collection of win/loss resolution from processors that don't readily support this data.
- **Dispute rules expert system:** Updates to the work queue will support more complex workflows, such as non-chargeback-related tasks like cancellation and blacklisting users. The queue will also support ongoing refinement of the evidence database depending on network rule changes.
- **Document generation features:** Performance improvements will be implemented.
- **Real-time resolution improvements:** Merchants will be able to implement decision logic based on customer, order, and product data when responding to real-time inquiries to more precisely control when credits are issued and inclusion of those details in the inquiry response.
- **Rules-based automation:** This functionality will include automated internal actions such as "ignore" or "note" by merchant based on certain criteria such as merchant ID or amount. Automated external actions will also be included, such as refund, cancel, note, or blacklist, based on similar criteria. This will also include automatic delivery of representment documents to processors.
- **Data analytics:** Merchants gain report visualization, including charts and graphs. Additional reporting options including order, usage, dispute history, "frequent fliers" (users who dispute transactions at a higher rate), and breakdown by product.
- **Dispute pattern analysis:** This includes the ability to score new disputes based on likelihood of winning and dollar value. Essentially it will prioritize "known losers" and time-wasters in a merchant's dispute queue.
- **Algorithmic dispute rules:** This will allow for an automatic decision regarding when to refund and when to dispute as real-time inquiries come in.

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.

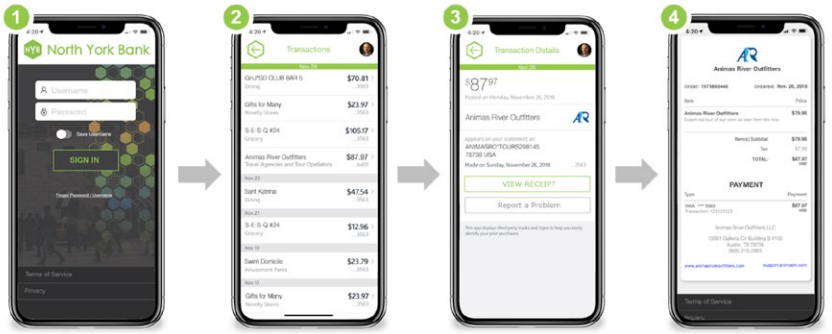
Ethoca's onboarding integration team works with customers to develop integrations. Merchants can code to the Application API and go live, which is the same for **Accertify** and **Kount**. The issuers integrate into a separate API, or may choose to provide intraday, file-based delivery to get data flowing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

paladingroup

Paladin 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.