# paladin vendor report | **fraud prevention**

paladinfraud


Thank you for downloading the Paladin Vendor Report.

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

The PVR, gathered by the industry experts at Paladin, provides detailed information on over 40 vendors who offer a wide variety of different fraud prevention tools, platforms, and services. This report is designed to give you a comprehensive overview of the different products offered by each company and present analysis to help you focus on who may ultimately best align with your individual fraud prevention goals.

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

Sincerely,

The MRC

# Table of Contents

## The 2021 Paladin Vendor Report

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

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

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

Since it's our mission to serve as an authority on these products and their strengths, areas of opportunity, and enhancements, we published the first-ever Paladin Vendor Report (PVR) in 2017. It offered an unprecedented exploration of how merchants could mitigate the risks that come with accepting payments in an omni-channel, card-not-present world. Because of the constant evolution of many popular fraud mitigation solutions, we decided to provide the Paladin Vendor Report on an annual basis. And now, we're pleased to publish the latest: the 2021 Paladin Vendor Report. We've offered previous participants the chance to update their sections and incorporated additional participating vendors.

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

**PRODUCT** - The vendor's current functionality.
**SERVICES** - Available offerings to help merchants during integration and throughout their client lifecycle, including reporting.
**BUSINESS DEVELOPMENT** - Current partnerships and channels for direct and indirect customers.
**MARKETING** - The verticals vendors are focusing on and messaging
**SALES** - A breakdown of market segments.
**TECHNOLOGY** - How the product works from a technical perspective.

# Introduction

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

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

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

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

- **User Behavior & Behavioral Biometrics**
- **3DS & Consumer Authentication**
- **Device Identification, Reputation, & Reputation**
- **Fraud Platforms & Decision Engines**
- **Identity & Data Verification**
- **Chargeback Management & Platform**

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

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 their proprietary Adaptive Behavioral Analytics and Automated Deep Behavioral Networks to model and predict real-time individual behavior. This functionality allows computers to understand when an individual customer's behavior is out of character; the platform then automatically evaluates the

FEATURE SPACE

OUTSMART RISK

### At a Glance:

risk. The technology can be deployed on-premise or via secure cloud, and it is scoring transactions from over 180 countries. In 2018, the **ARIC** platform risk-scored an estimated 15 billion transactions worldwide.

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

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** 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** Adaptive 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.
- Partnering 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.

## 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.

# Featurespace



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.
- **Fraud Market 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.

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 the 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.

# Neuro-ID

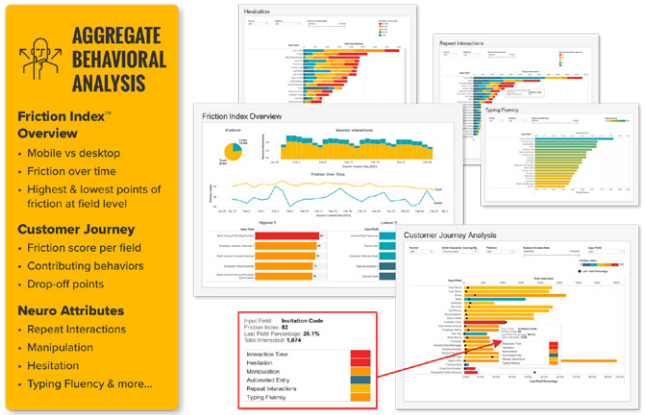


**Neuro-ID** is a behavioral analytics solution focused on separating fraudulent end-users from genuine ones within a digital customer journey. Via a lightweight JavaScript integration, **Neuro-ID** collects high-fidelity behavioral signals from web and mobile applications, processing these signals in session and making available scores (**"Neuro Confidence Scores"**) and attributes (**"Neuro Attributes"**) to inform real-time decisioning. **Neuro-ID's** scores and attributes offering is accompanied by a behavioral dashboard, which allows companies to understand and act upon end-user behaviors (behaviors indicative of intent—fraudulent or genuine—as well as emotion and experience) within their digital customer journey.

**Neuro-ID** helps clients focus on the following KPIs:

- Fraud rate
- False positive rate
- False declines
- Conversion rate

**Neuro-ID** operates primarily in the digital onboarding environment, account creation, account management, and account access. They are expanding rapidly into ecommerce and have a historical foothold in lending, payments, buy-now-pay-later, and insurance. The technology helps organizations "optimize friction"; through this process not only are bad transactions




NEURO-ID®
HUMAN ANALYTICS™ FOR THE DIGITAL WORLD

## At a Glance:

- 3rd Party API Capabilities
- Pre-Authorization Functionality
- ATO Detection Capabilities
- User Behavior Capabilities
- ATO Detection Capabilities
- Pre-Authorization Functionality
- Account/Client Management
- Device Fingerprint Capabilities

caught but more good transactions are identified and accepted. **Neuro-ID** partners with risk management teams by helping to move focus from cost center to revenue generator and, in many cases, aid in opening up additional market opportunities that are historically seen as high risk. Assisting both risk and experience teams, **Neuro-ID** uniquely enables companies to optimize conversion while reducing risk.

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

**Neuro-ID** is typically used as a layer in a larger stack. They help organizations "fill a gap" by going from strictly making decisions based on historical data to utilizing additional insight into behavior while interacting with the environment. Their (first of its kind) "friction dashboard" helps organizations measure and score customer friction and potential false positives. By going beyond fraud and risk tracking, the dashboard provides insights for a wide range of internal teams. These include marketing, customer experience, and even executive-level personnel. The friction index insights can indicate rates at which users leave the site, on which page, and which field—all the way down to session level.

As a real-time translation of "digital body language," **Neuro-ID's** proprietary scores and attributes reveal the "intent" behind behavior, also surfacing emotions of the online "experience." Derived entirely from in-session behavior, with no PII collected, this serves as a critical additive and orthogonal signal that is independent of outside data sources. Because of this, **Neuro-ID's** technology is effective for first-time applicants and customers with day-one value.

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

## Reporting options:

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

## Proof of Concept process:

**Neuro-ID's** Proof of Concept process begins with integrating the JavaScript for data collection. Reporting is made available via

# Neuro-ID



**Neuro-ID's** behavioral dashboard for understanding points of friction within a customer journey as well as behaviors indicative of fraud. Specific sessions are highlighted on a weekly basis for further analysis as part of the POC. **Neuro-ID** monitored 100M sessions in 2020, with a 500% year-to-year growth rate.

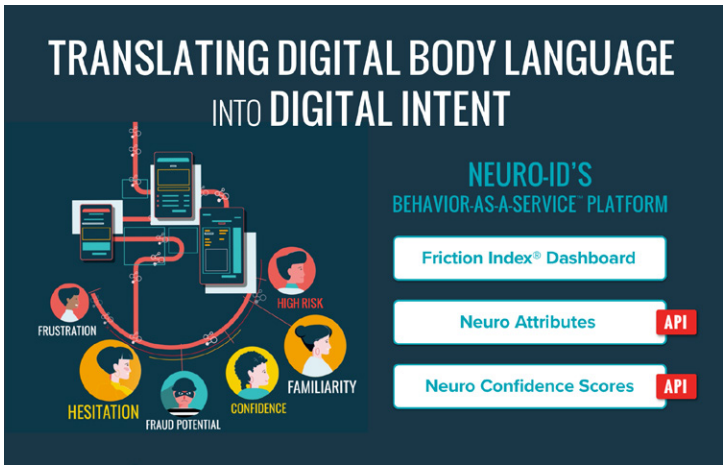
## Pricing format:

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

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

## Integration:

Integration with **Neuro-ID** consists of implementing a JavaScript snippet for data collection as well as integrating with **Neuro-ID's** API for retrieval of behavioral scores and attributes. Support for integrations is provided as part of customer onboarding, and there are integration guides for both the JavaScript and API integration. Level of effort for implementation depends on the capacity of the client but is typically completed within a couple of business days.




## 12-month roadmap:

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

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

# NuData

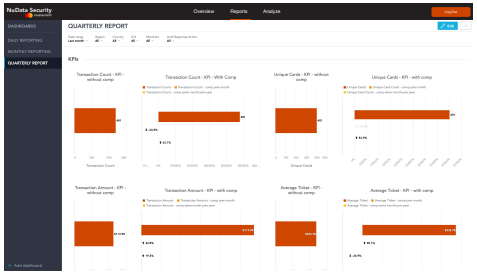


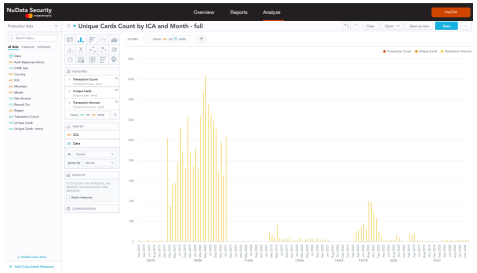
**NuData** is a Mastercard-owned company headquartered in Vancouver, British Columbia that specializes in device analytics, behavioral analytics, and passive biometrics. Since its inception in 2008, it has maintained a heavy focus on research and development while looking for better and more sophisticated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

The company's 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 hundreds of 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. Additionally **NuData** technology has been integrated into Mastercard's Risk Based Authentication Engine (RBA) as well as integrations in support of Open Banking standards.




**NuData Security**

mastercard

## At a Glance:

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

# NuData



## 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.

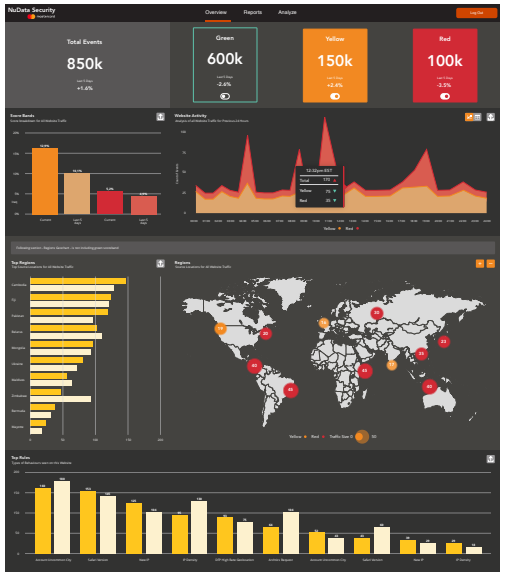
**NuData's** technology, and its **NuDetect** platform, are offered as a group of solutions, each targeted to specific industry pain-points and use cases. As such, **NuData** offers specific products that protect from automated attack risk (**NuDetect** for Automation), account takeover risk (**NuDetect** 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 (ATO) Risk:** With the vast amount of personal data readily available on the dark web, ATO attempts are on the rise. **NuDetect** for ATO helps protect against this threat, using behavior as well as a collection of additional data to validate legitimate logins and identify suspicious behavior. Individual account access is analyzed in real time to ensure there are no sudden changes in behavior that present risks to account security.

This can help clients by:

- Stopping scripted attacks at login
- Increasing confidence in customer interaction
- Reducing 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 high-value point in a web or mobile application. 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
- Mitigate human-looking attacks

# NuData



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

This can help clients by:

- Preventing future fraud from these accounts
- Avoiding fraudulent transactions
- Reducing operational costs
- Flagging human-farm-based account creation

**Frictionless user experience:** By utilizing passive biometrics as well as billions of behavioral profiles from **NuData's** Consortium, **NuDetect** for Good User Verification can help clients recognize legitimate users. It secures every point, from login to logout and at every interaction in between, even if account holders use autofill for their credentials. This can be used to provide users with an enhanced experience.

This can help clients by:

- Preventing false declines
- Building a relationship with good clients
- Removing unnecessary friction

**Device Recognition:** A subset of the **NuDetect** technology focuses on recognizing returning devices to prevent fraud and recognize trusted users without added step-ups. 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. Trusted Device will soon be integrated with all web-based products Mastercard is rolling out. And, post-upgrade, the benefits are immediate.

Future capabilities will focus on managing the risks and addressing the challenges associated with autonomous and semi-autonomous transactions coming from the ever-growing ecosystem of connected devices that make up the Internet of Things.

# NuData



**End-to-end visibility:** High-risk interactions can take place at numerous locations within a given application. For example, a user failing to login 30 times and then going on to make a purchase is very suspicious, but this can only be detected if the evaluation of these individual interaction points are monitored, and the resulting data is available for analysis within a common risk tool. **NuDetect** for Continuous Validation continuously monitors user behavior across the entire session, and provides functionality to identify these risks in real time.

This can help clients by:

- Preventing fraud at any step
- Detecting account hijacking
- Removing unnecessary friction on trusted users

**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 and hashed. **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, adding authentication step-ups only when the risk is high.

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

1. **Passive biometrics: 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, dwell time, key up/down analysis, accelerometer data, the way the device is spatially oriented, as well as other device sensor data that may be available. Passive biometrics allow **NuData** to achieve three key objectives.
   - First, determine if the user is human or nonhuman based on how the user is physically interacting with the device.
   - Second, if the user is a script, **NuData** can automate any action selected by the client.
   - Third, If **NuData** identifies that the user is a human, it discerns between the legitimate user or an illegitimate one, taking appropriate action.
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—perhaps a new version—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** identifies that Chrome has now jumped to 50% of the total traffic, it can look into the anomaly and find risk in real time that otherwise goes unnoticed. **NuData** analyzes hundreds of data points in real time across both the individual user and the 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 yearly. 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 selected 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 is also "the option for when the cloud is not an option." The company is recognized by AWS as PrivateLink Ready, a designation that allows **NuData** to offer its **NuDetect** product suite sending the data through a private connection instead of hosting it in the cloud, through the regular open internet. This offering is especially useful for companies subject to strict data protection regulations that can't process their data across the internet but still want to have a strong and real-time user verification process. 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?**

Every time a user interacts with the app or web platform, **NuData** evaluates the user's inherent behavior and other data to build a score and make a decision in real time. 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, device fingerprint, or device ID to analyze current and historical behavioral interactions across the full **NuData** network to identify anomalies and solve specific client use cases. The platform also allows clients to return real-time feedback, allowing the **NuData** models to further learn in real time.
- **Score: NuData** generates a numeric score that provides a risk value for the event profiled.
- **Score band: NuData** passes back a Green/Yellow/Red score-band identifier based on the total score generated for the event. The client decides what level of risk belongs they want to place in each score band.
    - **Unique device identifier:** Through the Trusted Device technology, **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. This includes the device ID, device fingerprint, and account history information.
- Real-time evaluation and customization: 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 clients 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, among others. 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:

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

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

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



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

## Account Takeover

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

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

## New Account Fraud

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

## Checkout Fraud

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

BehavioSec

### At a Glance:

ATO Detection Capabilities

Account/Client Management

Pre-Authorization Functionality

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

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

## Risk-Based Authentication

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

# DataVisor

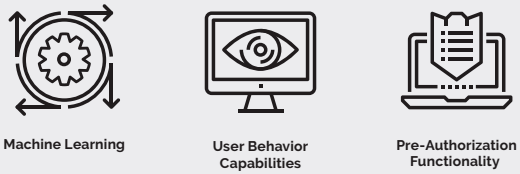


**DataVisor's** outlook is that fraud detection should be automated. Because of this, their approach to transactional risk mitigation is through unsupervised machine-learning technology. Unlike solution providers who rely on a machine-learning approach, they are using clustering technology to associate 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:




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:

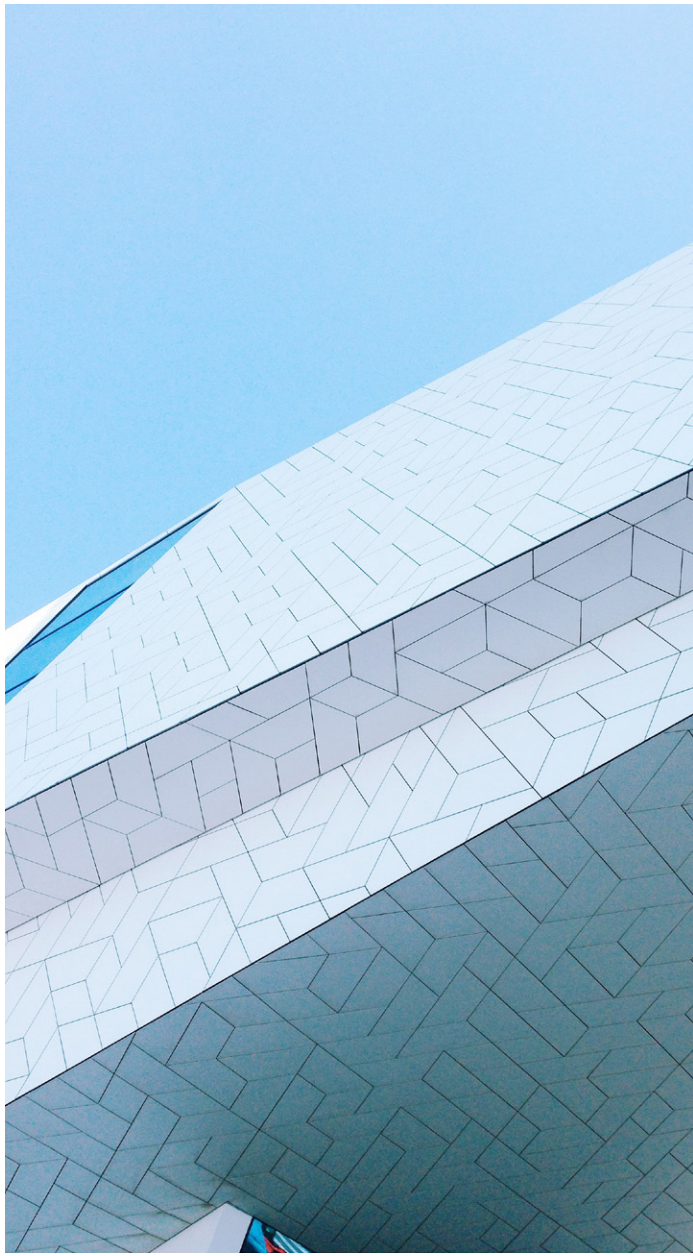
User Behavior Capabilities

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.

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



# Accertify 3D Secure



**Accertify** 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.

Accertify
AN AMERICAN EXPRESS COMPANY

## At a Glance:


## Accertify's 3D Secure (3DS) solution

**Accertify's** 3DS solution is available as a stand-alone authentication product or as part of their end-to-end authentication management solution. This 3DS solution supports both 3DS 1.0 (3DS1) and EMV 3DS 2.1 (3DS2). **Accertify** is currently certifying for 3DS2.2, slated for early 2021.

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

### The frictionless flow and the challenge flow

If the issuer authenticates the cardholder using only the data supplied in the 3DS message, there is no requirement for the cardholder to enter a password or PIN. This is known as the frictionless flow.

However, if the issuer is concerned about the payment, they can ask the cardholder to enter a password or PIN along with their card data. This data is entered into a separate window at the checkout stage, which is managed by the issuer. The merchant is not able

to view either the questions asked, or the responses provided. This is known as the challenge flow.

**Fraud liability shift**

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

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

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

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

# Accertify 3D Secure



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

**Merchant fraud strategy**

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

**Strong customer authentication (SCA)**

Furthermore, in Europe, 3DS has become the default solution for merchants who need to comply with new regulations like strong customer authentication (SCA). SCA requires that all intra-European Economic Area (EEA) transactions are authenticated by two of the following three factors:

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

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

While 3DS1 supports SCA compliance, the best way to meet SCA compliance is to integrate both 3DS1 and 3DS2. 3DS2 is a substantial improvement to 3DS1, and it provides the merchant with the ability to share more information about the payment and SCA-related information such as exemptions, mandated challenges, etc.

**Accertify** offers SCA Optimization to help merchants ensure regulatory compliance while taking advantage of SCA exemptions, ultimately helping to provide a positive check-out experience for customers.

# CardinalCommerce



For over two decades, **CardinalCommerce**, a Visa Solution, has been authenticating digital transactions for issuers, merchants, and processors around the world. As digital commerce grows and government mandates go into effect, authentication is becoming core to payment processing. With this shift comes more opportunities, and more challenges.

Cardinal offers access to faster, better decisioning, plus deep data that's intelligently connected. The **Cardinal Exchange** improves performance while protecting the customer from unnecessary friction, using more data for better insight into each transaction.

In selected industry verticals, there have been authorization increases of up to seven percent on authenticated transactions (vs. non-authenticated).[1] **Cardinal's** payment decisioning solutions help serve multiple players in the ecosystem, including merchants, issuers, and consumers.

Cardinal offers flexible delivery options for ease of integration, a rules engine to help optimize authentication strategy, and an expert support team to help along the way.

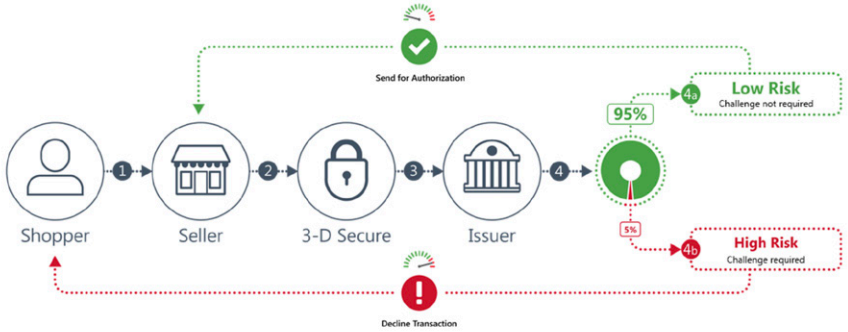
## At a Glance:


3rd Party API Capabilities

Pre-Authorization Functionality

Account/Client Management

## How it works




**Benefits of authentication**

Through shared data, merchants receive benefits like reduced false declines and fraud, increased authorizations, and improved customer experience.

**Cardinal** plays a key role in these benefits because of the **Cardinal Exchange**, which allows visibility into both sides of the transaction, from the issuer and the merchant. This adds up to significantly more information, a better consumer experience, quicker response times, and more control over step-ups, which can result in more authorizations.

When a consumer shops with a digital merchant and the merchant uses **Cardinal** for authentication, the process begins before checkout. More than 130 data points used for EMV® 3-D Secure can start to be collected while browsing (such as device intelligence).

Once the consumer checks out, the following will occur:

- Multiple data points, including transaction information, are sent to **Cardinal's** 3DS server, which formats and routes the data to the card network's directory server.
- The **Cardinal Exchange** connects data in real-time to help reduce fraud, increase approvals, and remove unnecessary friction from the customer experience.
- The issuer makes the risk decision, and the result makes its way back along the same path to **Cardinal** and the merchant. The issuer has the choice to either authenticate behind the scenes, ask the consumer to provide more information to their card-issuing bank, or decline to authenticate the transaction.
  - If more information, in the form of a challenge, is requested, Cardinal helps facilitate that between the issuer, the merchant, and the consumer.
- Once the authentication step is complete, the authorization flow begins.
- The merchant sends the transaction, with the authentication results, to their gateway and acquirer.
  - Standard authentication data includes electronic commerce indicator (ECI value) and cardholder authentication verification value (CAVV, AAV).
  - Additional data elements may be necessary, depending on the card network.

# CardinalCommerce

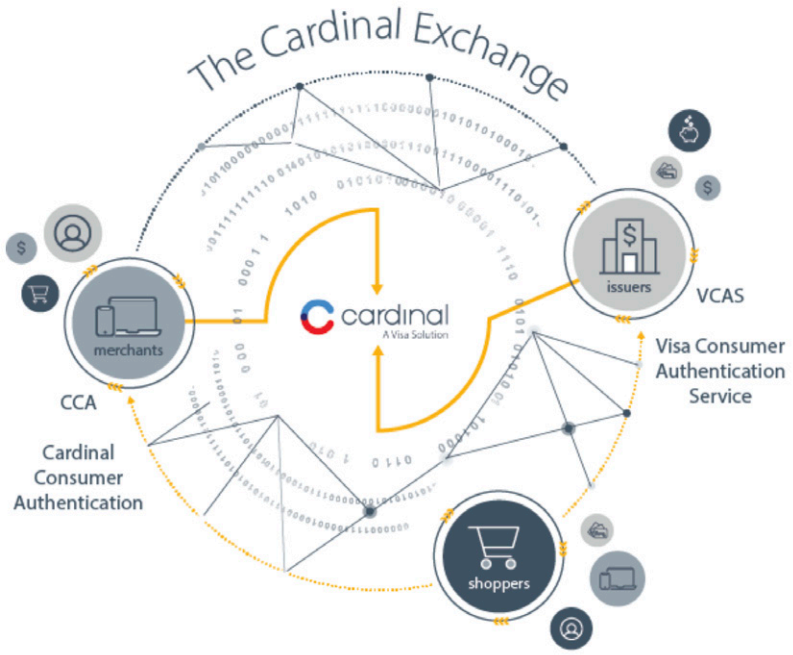


- The transaction is now sent to the card-issuing bank, which looks at the authentication information and confirms whether the consumer's account has sufficient funds to cover the transaction.
- The authorization decision follows the path back to the merchant.
- The transaction completes as authorized or is declined by the issuer.

The entire process takes place in milliseconds. The consumer often does not realize authentication is happening, unless their issuer challenges them for more information. With EMV 3-D Secure, when more data is shared between merchant and issuer, more transactions may be authenticated without challenges.

If a challenge is requested, that's not necessarily bad news. When the challenge is requested, authentication methods such as one-time passcode (OTPs) and biometrics are used to reinforce cardholder protection. As issuers get access to more data on the consumer's transaction request, including device and checkout information, only high-risk transactions should be challenged (unless the transaction is happening in a regulated region where two-factor authentication is required).

The **Cardinal Exchange** connects data in real-time to help reduce fraud, increase approvals, and remove unnecessary friction from the customer experience. **Cardinal** powers a large global authentication network for digital commerce, including tens of




thousands of merchants and thousands of issuers running billions of transactions a year. **Cardinal** is focused on continuous improvement and investment in market demand.

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

## Merchant products

3-D Secure and authentication solutions:

- **Cardinal Consumer Authentication:**
  This is a data-driven solution designed to enable merchants to improve the authentication experience. The 3DS program can help increase approved sales and reduce fraud. This includes the card networks' EMV 3DS programs like Visa Secure and Mastercard Identity Check.
- **Data Only:**
  It's tricky to find a balance between maximizing good transactions and reducing the amount of false declines with minimal friction and latency. Cardinal's Data Only solution works with both Visa and Mastercard and is focused on improving authorization decisions and maximizing speed when not hypersensitive to fraud. Using the EMV 3DS rails, merchants can share data with issuers with a guaranteed frictionless experience, and no liability protection.

**Features to help merchants today and in the future:**

- Cardinal's dynamic routing features, including 3DS replay:
  - When the merchant has adopted EMV 3DS but the issuer hasn't, 3DS replay helps preserve liability protection for merchants. When an EMV 3DS transaction results in an error or attempts, or the ACS is not available, 3DS replay steps in and runs the transaction as 3DS 1.0. The merchant retains liability protection, and in the EEA, where authentication can be required for SCA, there is less chance that the transaction will be declined without authentication.
- Mastercard Identity Check Express Support:
  - Mastercard's Delegated Authentication solution, which allows merchants with their own authentication capabilities to stand in and authenticate transactions on behalf of the issuer.
- Travel Industry Message Extensions:
  - These provide additional data on the EMV 3DS messages for use by travel-focused merchants to help issuers with the context of the transaction. Not only has **Cardinal** added support for these fields to our API, some of these data points have been added to the rules engine, for control over authentication strategy.
- Support for all major card networks:
  - EMV 3DS v2.1: Visa, Mastercard, American Express, Discover, JCB, Union Pay, ELO (Brazil), Cartes Bancaire (France).
  - 3DS 1.0: Visa, Mastercard, American Express, Discover, JCB. (Note that Union Pay, ELO and CB do not offer 3DS 1.0).
  - EMV 3DS v2.2: **Cardinal** currently supports Visa; all other networks are in progress and expected to launch in 2021, along with new regional networks.

**Issuer products**

- Visa Consumer Authentication Service (VCAS)
  - VCAS, **Cardinal's** issuer ACS, uses real-time risk-based assessments across all major card networks, giving issuers the power to change with the payments landscape. It gives issuers the ability to create, test, and publish authentication rules from **Cardinal's** convenient portal.

**Issuer features**

- **Compliance manager:** Designed to help issuers in the EEA when they are managing SCA. This solution helps manage by ensuring proper separation of policy and rule types in a user-friendly application.
- **VCAS risk model updates:** Updates to the VCAS risk model help assess the risk of digital transactions during authentication based on hundreds of data points. The model uses machine learning to identify patterns in past transactions, to then apply learnings to future authentication requests.
- **Rules tester for EMV 3DS:** Ability to test EMV 3DS risk rules before publishing them into production.
- **One-Time Passcode + Knowledge-Based Answers:** Ability to step-up with OTP & KBA to help meet the PSD2 SCA mandate in the EU region.
- **UnionPay International and JCB on EMV 3DS (version 2.1):** Network certification to support EMV 3DS program on VCAS
- **Confirmed marking multi-select:** Update to support marking multiple transactions (good, fraud, undetermined) at one time within the VCAS portal Reporting Application

**Cardinal support network** offers in-region local support, anchored by Cardinal's team of product experts and 24x7x365 online support site.

## Cardinal's approach to PSD2 SCA

**Cardinal** has focused on PSD2 SCA requirements since the initial Regulatory Technical Standards (RTS) were issued by the European Banking Authority (EBA) in 2017. By partnering with EMVCo and the card networks, they aimed to build a better ecosystem.

Products for issuers encompass a wide range of PSD2 SCA related offerings:

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

# CardinalCommerce



As issuers integrate these tools, merchant partners are able to improve consumer authentication experience through compliant SCA methods. They begin to use exemption capabilities to reduce the rate of SCA consumer presentment.

The **Cardinal Consumer Authentication** (CCA) product for merchants supports the necessary EMV 3DS version 2.2 message format (to request exemptions via the values contained within the 3DS Challenge Indicator and other supported fields such as 3RI, Non-Payment, and others). Since 2015, they have offered a flexible rules engine, allowing merchants to choose to control the exemption requests themselves within their message format or via the Centinel Rules Engine.

**Cardinal** supports Visa Delegated Authentication and Mastercard Identity Check Express. They also work closely with Visa to enhance the product offering for Visa Delegated Authentication by offering several value-added features to issuers and merchants. The end goal is to provide an improved SCA experience by allowing merchants to perform SCA and allowing issuers to approve those authentications in real time. The key pillars of focus are transaction processing speeds, mass issuer adoptions, and the best cardholder experience.

**Cardinal** works with:

- 7 of the Internet Retailer's Top 10 merchants[2]
- 6 of the top 10 U.S. credit card issuers and 6 of the top 10 U.S. debit card issuers[3]
- Over 20 processors that serve issuers and over 100 processors that serve merchants around the globe[4]

## 12-month road map

- EMV 3DS version 2.3.0 support
  - **Cardinal** is an early adopter with EMVCo, and will be working on their version of the solution for both issuers and merchants as soon as the specs are released
- Support for additional payment networks around the world
- Additional API integration providing BIN-level insights related to authentication capabilities and performance
- Behavioral biometrics to help meet the PSD2 mandate in the EU region
- Dashboard for real-time KPI and performance monitoring within the VCAS issuer portal



[1] Source: Cardinal and Visa data. Statistics are drawn from the latest available data covering the period Nov 2017 to Nov 2018

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

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

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

**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.

# 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 allow clients to address risk pain points across the entire customer journey. From account creation to authentication, activity monitoring, payment, and disputes, risk is mitigated without impacting the customer experience.

## Solutions and Functionality

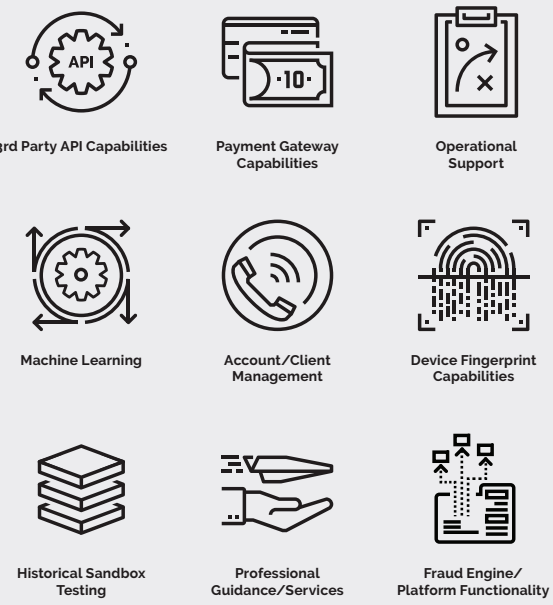
The **Accertify Interceptas® Platform** is a software-as-a-service offering that allows clients to customize and adapt their fraud-screening strategy in real time, leveraging best-in-class industry machine-learning models, configurable fraud and policy rules, and robust reputational community data. The 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 data providers. The platform is PCI-DSS Level 1 certified and is SOC2 and ISO 27001 compliant.

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

**Scoring Functionality:** At its core, the Interceptas® Platform is a data-management tool. By offering a rich set of integrated machine-learning models, 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

Accertify
AN AMERICAN EXPRESS COMPANY

### At a Glance:



to third parties or leverage **Accertify's** rich sources of community data.

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

In 2020, **Accertify's** Case Management evolutions centered on a few key themes, including:

- Improved navigation and user experience (UX) enhancements.
- Continued investment in industry-focused machine learning models.
- Multilayered search and visualizations were released; these allow analysts to easily and efficiently find out-of-pattern behavior, fraud rings, and new trends. In addition, this new functionality includes a network graph and timeline–a visual approach to showing connections across transactions.

**Machine Learning Powered by Dynamic Risk Vectors:** Machine-learning capabilities power the creation of **Accertify's** 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 your transaction decisioning outside of your business interactions.

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

**InMobile** provides a software development kit (SDK) that can be incorporated into mobile applications to access detailed mobile device information. More than 100 device attributes and operating system attributes can be collected and analyzed to produce a persistent device identifier that is resilient to tampering, application uninstall/reinstall, and OS upgrade.

Core features include:

- **Malware and Crimeware Detection:** InMobile analyses connected devices to detect known malicious applications as

well as criminal tools, such as location spoofing and IP address proxy apps. Malware files are dynamically updated without client interaction.

- **Rooted/Jailbroken Detection:** InMobile protects against increasing and complicated rooting methods used by fraudsters, such as cloaked Root, through Advanced Root and Jailbreak Detection.
- **Trusted Path:** Trusted Path is InMobile's security architecture, preventing interceptions by providing a complete secure path to transport sensitive information. The information is encrypted end-to-end, signed, and digitally protected against replay attacks. InMobile uses Trusted Path to securely communicate sensitive messages
- **Secure Messaging:** This is a secure means of delivering contextual two-factor authentication (2FA) messages to a registered device through the InMobile SDK and secure Trusted Path. The messages cannot be read by any other device, intercepted, or replayed. This can be a stand-alone offering.

**InBrowser** provides JavaScript collectors that can be incorporated into any relevant web page to access detailed browser session information. Hundreds of attributes can be collected and analyzed to produce a persistent device identifier and identify potentially fraudulent behavior. Collector code can be invoked upon page visits 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 the account open page, login page, account change/update page, and checkout/payment page.

- Our browser fingerprint "recipe" determines how well devices are differentiated from each other. This allows any client to seamlessly authenticate users with less friction by minimizing collision rates and maximizing fingerprint longevity.

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

**Link Search Capabilities: Accertify's** enhanced link search functionality gives clients the ability to search for historic linkages that can clarify whether an event is out of pattern, or whether there is evidence of a loyal, repeat customer. The capability is flexible regarding which values can be displayed and searched. And it 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 functionality provides the ability to look historically and get an analysis of a proposed rule change. For testing conditions on current and future transactions, a client can run tests in the production environment and set a passive score where it wouldn't affect the outcome. Production testing gives clients the ability to run transactions through "real-world" conditions such as velocity and negative files.

**Profile Builder:** Profile Builder helps identify real-time patterns and trends through the dynamic summarization and aggregation of data. Gain insight in real time at the transactional level to discern fraud rates, track new product launch limits, monitor account usage, analyze customer buying patterns, and uncover organized fraud rings. No longer is it necessary to anticipate potential risk, wait overnight for a model or algorithm to be updated or calibrated, or use static, stale rules. In real time, Profile Builder monitors summarized fraud rates at the product/sku level, across airline route networks, at events/locations, against a specific entertainment genre, or any number of similar entities, thereby easing manual review rates and enabling a more efficient and flexible strategy to mitigate risk.

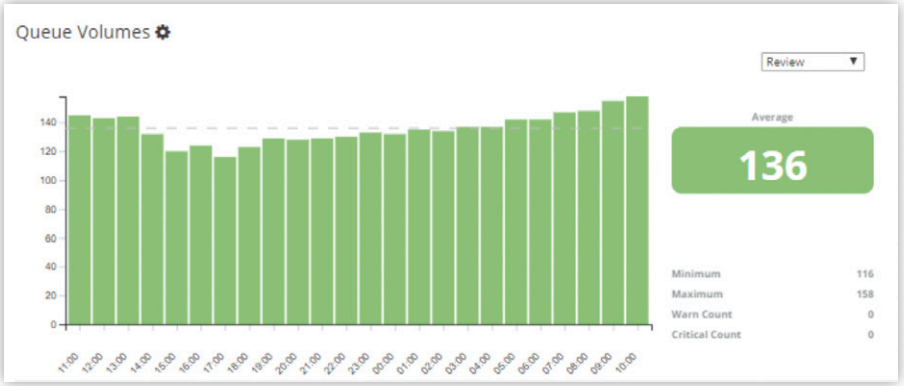
**Chargeback Management:** Please see the full write-up in the Chargeback section of the Paladin Vendor Report.

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, and it provides easy connectivity to multiple acquirers globally.

## Reporting:

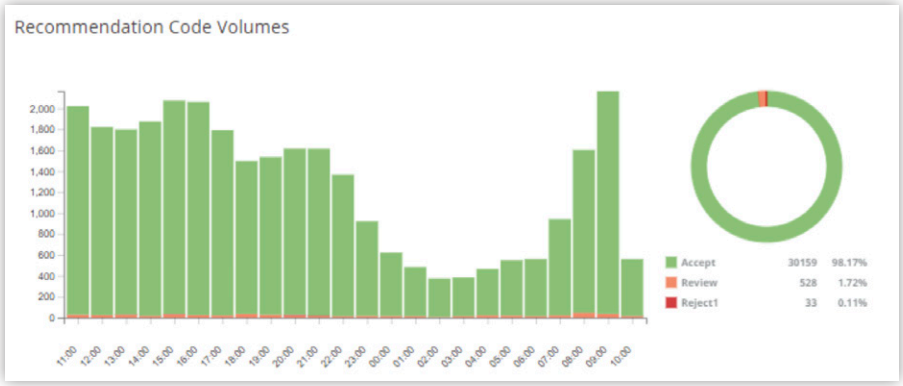
Accertify offers three types of reports:

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

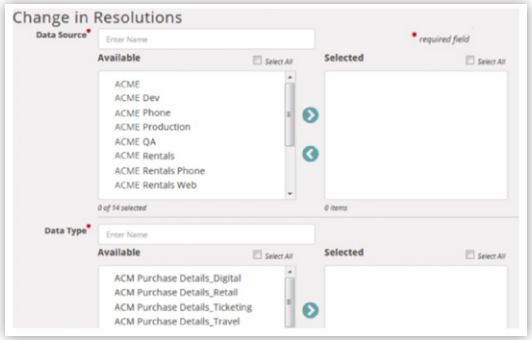


# Accertify, Inc.

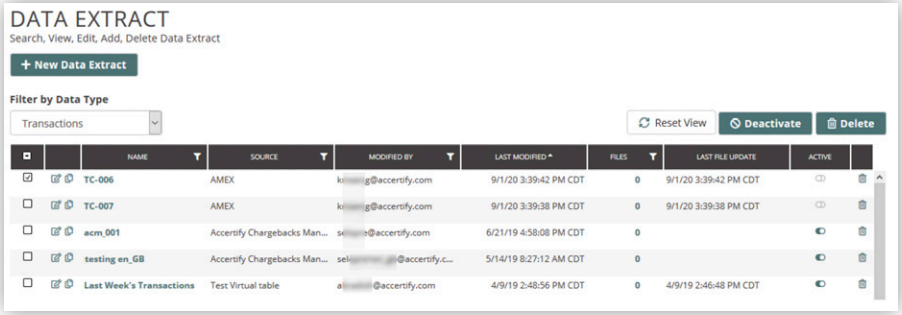



- **Enterprise Reports:** These allow a client to input criteria parameters to specifically drill down and show different types of performance. Examples include monetary metrics, chargebacks, analyst decisioning, rules performance, and more.




- **Data Extract Utility:** This reporting suite allows clients to create either one-time or recurring scheduled reports where they can extract large amounts of data. Reports that are generated via the Data Extract Utility feature can be securely exported onto the client's systems where they can use their own software to look for trends or report to their own internal teams. More advanced features include data pivots and exports to Excel format.




## 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 an unparalleled network of reputational community data, to provide clear, defensible reason codes that detail insight into the factors driving the model decision.
- Listening to our clients' needs, sharing insights, and designing a set of machine-learning-based solutions to address their needs.

# Accertify, Inc.



- 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): Accertify's** global team of Client Success Managers are responsible for ensuring each client is achieving their fraud and chargeback goals. The Client Success Team primarily comprises former Directors and Managers of Fraud from the most recognized brands in the world. They possess extensive first-hand fraud and chargeback experience, along with a deep understanding of the **Accertify** Fraud and Chargeback Platform. They know directly how it can be deployed to solve complex challenges. The team stays closely aligned internally to ensure clients are aware of new features and functionalities, and they work with clients to help them adopt those features and functionalities within their environment to achieve the maximum benefit.

**Managed Services: Accertify's** Managed Services team provides direct operational management of clients' fraud and/or chargeback processes leveraging their industry-leading Interceptas platform. The team works hard to serve as an extension of clients' organizations by providing experienced and comprehensive consultation, geographical coverage, and SLA management. Clients get the extensive resources they need while driving lower costs and overhead, increasing efficiencies, and peace of mind.

## 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. By completing rigorous platform and technology training, their multilingual team's extensive fraud prevention, chargeback management, and client success experience ensures excellent outcomes. They provide quick 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 more.

**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 is made up of 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.

# ACI Worldwide (ACI Fraud Management)



**ACI Worldwide** delivers real-time payment solutions that power in-store, ecommerce, and mobile payments while managing fraud and risk. The company supports merchants and Payment Service Providers (PSPs) to help them meet the real-time payment needs of their consumers and business customers.

**ACI** is committed to innovation and continuous solution enhancement through significant investment in research and development. This ensures that the company's technology, services, and advice continue to provide demonstrable benefits to its customer base of over 80,000 merchants, whether they're served directly or through PSPs.

## Solutions and Functionality

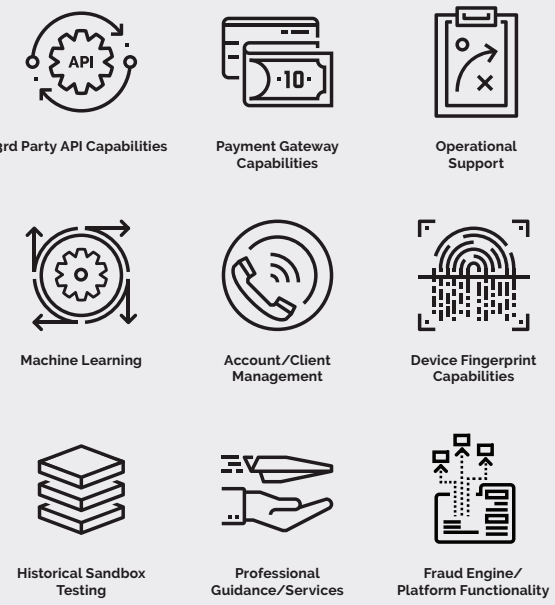
**ACI Omni-Commerce** provides end-to-end payments and risk management services to in-store merchants and card-not-present ecommerce merchants across a variety of verticals, including telecommunications providers, retail, grocery, gaming and entertainment, digital goods, travel and hospitality, fuel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

Within **ACI Omni-Commerce**, the **ACI Secure Ecommerce** solution includes a global ecommerce payments gateway and a robust, multilayered ecommerce and m-commerce fraud management functionality.

**ACI Secure Ecommerce** serves as a bank-independent, acquirer-agnostic "one-stop shop" letting merchants manage just one relationship to secure an independent payments gateway with fully integrated fraud prevention. This makes possible a multitude of acquirer and alternative payment offerings through a single API connection. Merchants and PSPs can remain in control of their acquiring and alternative payment

ACI Worldwide
Real-Time Payments

### At a Glance:



relationships and associated commercials, all without having to establish and manage multiple relationships to fulfill their payments processing needs. (Additional details related to the payment gateway can be found via the Paladin Payment Vendor Report.)

As part of the **Secure Ecommerce** offering, the flexible, multichannel **ACI Fraud Management** solution is fully integrated into the payment flow for both pre- and post-auth screening via the same single API. This, along with performance metrics and active/active architecture, gives the customer the scalability and flexibility to "sell more and lose less," focusing specifically on achieving:

- Increased checkout conversion rates, resulting in additional revenue with no negative impact on fraud rates or chargebacks
- Optimized payment acceptance options from 250+ different acquirers and APMs including Apple Pay, Android Pay, Pay Later providers, and digital wallets
- Reduced false-positive rates and strategies adaptable by country, region, channel, payment type, and product type
- Reduced operational costs

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

**New in 2020**

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

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

## ACI Fraud Management: A Multilayered Approach to Fraud

There is no silver bullet to mitigate fraud and achieve high conversion rates while keeping chargebacks in check. This is why **ACI** deploys a multilayered approach, combining multiple tools and technologies, automation, and human intervention to manage fraud while focusing on conversion. The solution uses machine

learning and profiling combined with a series of real-time alerts and dashboards. They give merchants flexibility and control over their strategy, with support from a strong team of expert risk analysts and data scientists. Fraud strategies can be modeled to the requirements of each customer (direct or indirect) and adjusted in real time.

**Retrospective Alerting**

The solution not only decisions in real time but also alerts merchants to changes in transaction risk status (post acceptance) in response to new negative/fraud intelligence. The solution allows retrospective "continuous" screening on all transactions across all distribution channels, geographies, product types, and payment types. As an example, if ACI receives negative information on a transaction after it was approved, the merchant can be notified to cancel or re-route the shipment.

The solution's self-service business intelligence portal provides visibility into the merchant's transactional data and decisioning rationale, allowing the merchant to monitor key performance metrics and proactively refine the fraud prevention strategy.

**The Multilayered Solution in Detail**

- **Machine Learning**

  **ACI** supports and develops multiple machine-learning model options including custom models, merchant-specific models (for larger merchants), and over 15 vertical-focused models (including telco, travel, retail, gaming, and digital). Over 7,000 features are used to create **ACI** models, ensuring high performance regardless of sector. In 2021, **ACI** will launch an incremental learning algorithm (patent pending), a fully automated unsupervised model that auto-adjusts in response to new data intelligence. This reduces degradation in effectiveness as well as the need for often costly model refreshes. Models are supported by a dedicated team of data scientists. With ACI's consortium of shared fraud intelligence data, every merchant reaps the benefit of models that have been trained on high volumes of industry-specific data that are added to daily. This ensures consistent and reliable performance over long periods.

- **Profiling**

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

# ACI Worldwide (ACI Fraud Management)



- **Link analysis**
  This identifies data points associated with a confirmed fraudulent data point, allowing visibility into patterns of emerging fraudulent behaviour.
- **Autopilot**
  Based on high-efficiency rules for a specific period, real-time responses are monitored and associated order elements are automatically blocked.
- **Auto-Analyst**
  An auto-analyst function allows further automated investigation outside of the real-time decisioning window. The auto-analyst function is a useful additional layer in the strategy and can be enabled to scale rapidly and in response to increasing volumes when fraud review teams may be under pressure. Auto-analyst can also be used to fast-track time-sensitive transactions such as "same-day" or "next-day" delivery or "buy now / pick up in store" orders.
  Challenged transactions (often flagged for manual review) can be automatically routed to third parties (via an integrated third party orchestration layer) for additional validation or verification, leading to a firm, automated accept or deny decision.
- **Tumbling and swapping**
  Tumbling and swapping rules (TSW) identify transactions where cards or emails have been manipulated by making small adjustments to the data (for example, if a user changes the last four digits of the card or adds a number to an email).
- **Rule category flags**
  Additional codes accompany the accept/challenge/deny response back to the merchant. Rule category flags map to a rule (or group of rules) and provide the merchant with more details on the recommendation as part of the response string.
- **Silent mode for rule testing**
  Rules can be applied to run in parallel through silent mode for a period before applying to active mode (production), such as in champion/challenger strategies. This allows merchants to test the effectiveness of a rule and optimize it without impacting live customer transactions.
- **Enhanced response**
  Get additional information, such as the reason for the response given alongside the elements contributing to the result. This can be incorporated into a merchant's (or partner/PSP's) own user interface and internal platforms.
- **Fuzzy matching**
  "Fuzzy matching" pattern recognition functionality helps identify linked fraudulent attempts in which address concatenation/manipulation and/or email tumbling might appear as unique transactions to most automated systems. This makes it easier to identify fraud trends and enables fast mitigation action.

# ACI Worldwide (ACI Fraud Management)



- **Third party orchestration**
  One integration and one contract with **ACI** gives merchants access to multiple third-party providers. Users can pick and choose the options that make most sense for the business. Third-party callout results are accessible through the interface, providing integrated and automated connectivity to specialist third-party partners. This provides even greater detection capabilities as well as additional data insights to assist decision making. To manage costs, **ACI** utilizes smart routing functionality so transactions can be qualified in or out for third-party callouts. **ACI** can automate connectivity and receive responses in real time to incorporate into the overall core strategy and influence final decisions.
- **User support**
  - **Risk Analysts: ACI's** global team of dedicated risk analysts are an inclusive part of the **ACI Fraud Management** service. Analysts cover four continents (and 15 languages) and have access to global payments intelligence and local market knowledge. They average five years of experience and many are certified ecommerce fraud professionals. All have degrees in math, computer science, or data science. At the start of an engagement, risk analysts collect in-depth merchant background information including historical fraud data. They review existing processes and operations and identify a potential strategic approach.
  - **Data Scientists: ACI's** dedicated team of highly skilled data scientists have more than 120 years of experience between them, and are all educated to MSc and PhD level. The team is responsible for both AI and machine-learning strategies across **ACI's** portfolio. They have over 15 consortium models in production, covering all main verticals from retail to clothing, gaming, and travel. The team continues to innovate, bringing new technology to market, preventing fraud, and helping customers utilize machine learning in a meaningful way. The team is multilingual with representation in the US and Europe. Academically, the team is well published and has over 30 publications between them, continuing to contribute to the ever-evolving domain of data science.

## Administrative tools

**Control Center:** A single-sign-on interface provides access to the customer service interface, Case Manager, Feature Manager, List Manager, and Business Intelligence tool. It gives users access to decisioning rationale on individual transactions, including order data points, response, and rule description explanation. Color coding of decisioning responses increases visibility of high-priority risk indicators.

# ACI Worldwide (ACI Fraud Management)



**Business intelligence:** Within ACI Fraud Management, a business intelligence (BI) dashboard and reporting tool provides visibility into all activities and includes two years of transaction history. The tool continuously tracks key performance metrics associated with rules, profiles, retrospective alerts, false positives, etc. It can help identify new and emerging high-risk trends. The tool also allows users to develop, test, deploy, and monitor rules in active or passive/silent mode. Merchants can view fraud KPIs such as accept, challenge, and deny rates, plus trends on a global and channel basis.

**List manager:** A new feature in ACI Fraud Management enables merchants to create lists that can be referenced in rules, such as lists of bad IPs or known good email addresses. The feature can be used for positive or negative lists.

**Rule manager:** It uses features and lists, allowing merchants to add, delete, and modify rules in real time.

**Feature manager:** Create multidimensional features (sophisticated sets of instructions incorporating several data points, conditions, and calculations) or use a template library of predefined features. Users can deploy multidimensional rules and complex rules at the click of a button. This removes the need to build rules from scratch, and one feature can achieve an outcome that removes the need for multiple rules.

When coupled with the new rule manager and list manager, merchants can use the feature manager to create customized conditions, features, and lists to significantly enhance "allow" decisioning for good customer acceptance and to further minimize false positives.

**Block manager:** Merchants can create positive or negative lists on any data point sent as part of the transaction.

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

## Support Services Offered

Merchants are assigned a designated Customer Success Manager (CSM) and Risk Analyst (where appropriate).

**Fraud performance management:** Ongoing, regular meetings are held with the designated ACI risk analysts and assigned data scientists, who will review key performance metrics and make recommendations to enhance the strategy.

**HELP24 Support:** Support can be reached 24 hours a day, seven days a week, 365 days a year, to answer product questions and resolve technical support issues.

# ACI Worldwide (ACI Fraud Management)



**Manual order review:** Merchants are provided a team of support analysts to manually review challenged transactions and make final decisions. Decisioning accuracy is tracked and monitored to ensure key performance indicators are met. Service can be deployed in general BAU or at peak times only.

**Chargeback representment:** An outsourced chargeback representment service manages chargebacks and representment process facilitation.

**Chargeback indemnification:** A service offered to selected customers.

## Integration Process

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

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

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

**In development over the next 6-12 months**

2021 will bring a patented incremental machine-learning capability, which allows for fully automated incremental learning models. These will remove the need for expensive and time-consuming model refreshes and allow faster new model deployment. Machine-learning scoring visualization will also be enhanced.

Other enhancements will include:

- **ACI strategy impact analysis:** the ability to test strategy impact logic by running against historical data (note: this facility is in addition to the silent mode function that tests strategy in silence against production data).
- **BI tool enhancements:** self-service reports with self-design and improved export facilities.
- **Enhanced data responses:** raw data feedback mechanism detailing data and decision rationale for ingestion by a PSP, acquirer, or a merchant's own portal or dashboard.

# ACI Worldwide (ACI Fraud Management)



- **Additional third-party partners:** added to a third-party orchestration layer.
- **Enhanced data sources:** Including an improved ability to capture data from sources such as social media.
- **Automated rule detection:** More and more information is necessary for decision making; ACI's Artificial Intelligence will make rule recommendations based on detected patterns.
- **Unsupervised learning:** The ability to infer the natural structure of the data, discovering hidden patterns and detecting anomalous behaviors. The newly discovered patterns are used for feature creation and to identify fraudulent behaviors, strengthening the customer's fraud strategy.
- **Graphical link analysis:** To discover connections between different customers, identifying criminal or suspicious activities that uncover how fraud rings operate—and allowing for a continuous and efficient way of blocking organised fraudulent activities.

# ClearSale



**Clearsale's** fraud solutions combine advanced technology with a team of experts who understand their clients' unique needs. **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:

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

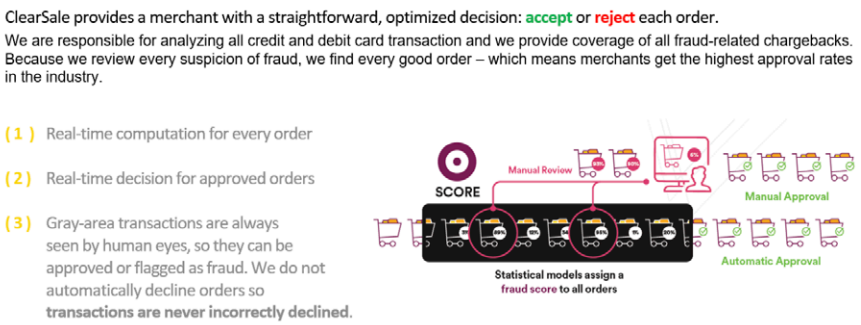
| | | |
|---|---|---|
| **99%** Retention rate | **4,000+** Direct clients | **19+** Years in the market |
| **1,000+** Fraud analysts | **160+** Countries | **24/7** Availability |

With over 19 years of experience and a presence in Australia, the United States, Brazil, Mexico, and Argentina, **ClearSale** maintains a global footprint. **ClearSale** boasts over 2,000 employees and over 4,000 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 conducts 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



**ClearSale** takes pride in guiding clients through the process design to the script for manual reviews and reports. Their business model is based on performance and the flexibility to adapt to a variety of business needs.

| You Know | Clearsale Can |
|---|---|
| Your most profitable products | Prioritize these products across the analytical process. |
| Your customer preferences in different countries | Provide custom fraud prevention in accordance with inherent fraud differences across the globe. |
| Your general customer profiles | Develop procedures to support your customers in the most appropriate ways. |
| Your VIP customers | Tailor our playbooks to offer a higher level of support. |
| Your target markets | Provide industry-specialized fraud analysts, available 24/7 with multi-language capabilities. |

**Clearsale's Mission Has Five Main Objectives**

- **Prevent fraudulent activity: ClearSale** originated in the dynamic ecommerce environment of Brazil 19 years ago—and their experience in high-risk markets has allowed the company to develop processes that find and mitigate against fraudulent tactics.
- **Maximize conversion and minimize falsely declined transactions: ClearSale** recognizes the severity of the false decline problem, not only due to lost revenue, but also loss of the customer lifetime value (CLV). 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.
- **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.
- **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.
- **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: ClearSale** works with the merchant to define a quarterly chargeback threshold that **ClearSale** commits not to surpass. Clients are billed on approved transactions. If **ClearSale** does not meet the chargeback threshold, **ClearSale** offers a predetermined discount on the merchant's quarterly invoice..
  - 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:

- Retrieve the plugin
- Enable the **ClearSale** module within the store
- Keep track of the orders on the **ClearSale** dashboard

The **average integration time** is eight working hours if a merchant follows the API guide, and can be reduced to one hour if installing via a platform plugin. ClearSale has plugins with many of the major platforms, including (but not limited to):

Magento
BigCommerce
WooCommerce
Shopify
Volusion
PrestaShop
Oracle Commerce Cloud
Sales Force Commerce Cloud

## 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** is certified according to the security standards stated by the PCI DSS information security standard and follows all of the data security best practices established by ISO 27001.

**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.

# Cybersource



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

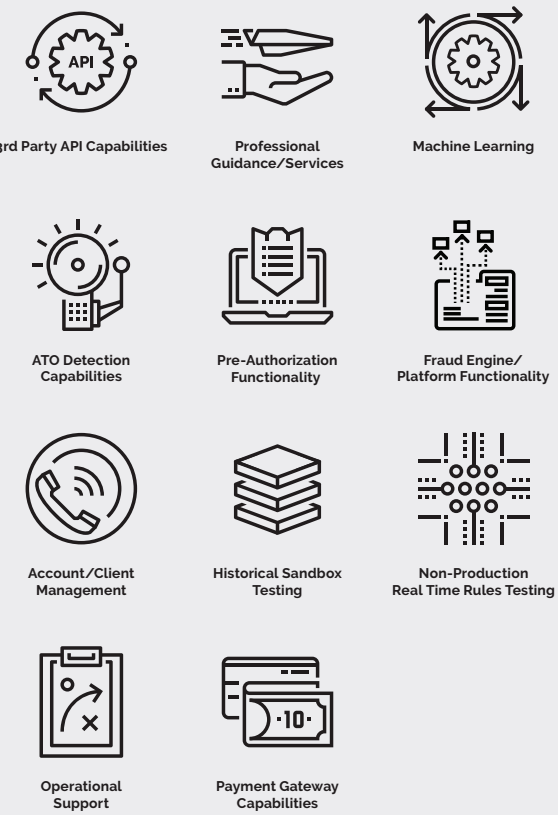
Decision Manager (DM) is their flagship enterprise-level risk management solution that helps manage fraud and increase customer satisfaction. Decision Manager allows businesses to make risk adjustments to stop fraud before it starts, and it helps detect more good orders quickly. This delivers greater insights for businesses and adds value to every transaction. The Unified Consortium model stays current with emerging fraud patterns by combining regional, industry and vertical Decision Manager data to provide frequent model updates, optimize accuracy with various detection tests, a fully customizable rules engine, case management capabilities, and real-time reporting.

## Decision Manager Capabilities

Once integrated, the Decision Manager fraud management tool provides machine-learning results on all transactions processed. This is most commonly used by merchants in the form of a score (scored on a scale of 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 tool utilizes both static and dynamic machine-learning technology designed to enhance the capabilities of their rules engine. The solution

cybersource
A Visa Solution

## At a Glance:



offers more than 260 automated validation tests and is enhanced by 141 billion worldwide transactions processed by Visa annually*.

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

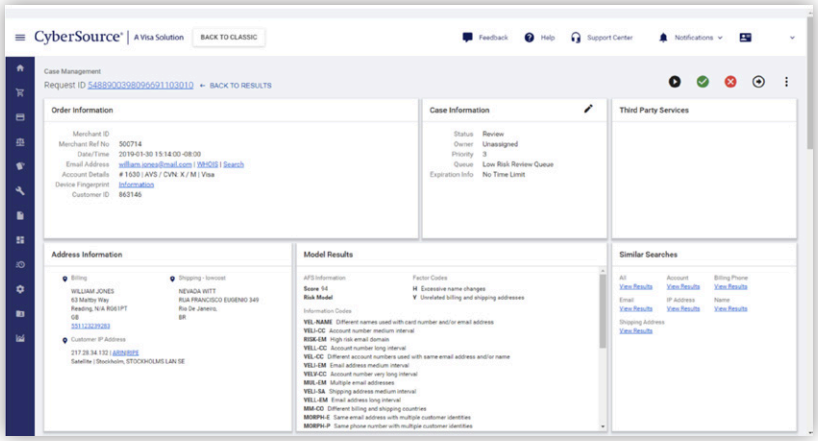
- **Information on excessive address changes:** For example, if the customer changed the billing address multiple times or used multiple credit cards within a certain time frame.
- **Tracking of identity-morphing behavior:** Decision Manager can find multiple values of an identity element that are linked 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, alerting if the customer's account number was used many times in the past 15 minutes. Decision Manager also can expand on velocity behavior by providing global validation of specific velocity use, such as account number, email, addresses, or IP address all being used in a short, medium, or long tracking interval.
- **Behavior surrounding customer input:** This is collected and analyzed, and it can provide details such as nonsensical input, repeated characters, and input data.
- **Utilization of advanced device behavior and fingerprinting:** This helps identify good customers based on their interactions with a merchant's website.

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:

Callouts to third-party validation services such as Emailage, ThreatMetrix, Ekata, CardinalCommerce, and Neustar.

- 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.

*VisaNet transaction volume based on 2020 fiscal year. Domestically routed transactions may not hit VisaNet.




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.

Device behavior attributes such as copy/paste recognition and mouse, keyboard, and screen analytics can be used in Decision Manager and Account Takeover Protection to help identify good customers based on their interactions with a merchant's website.

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.

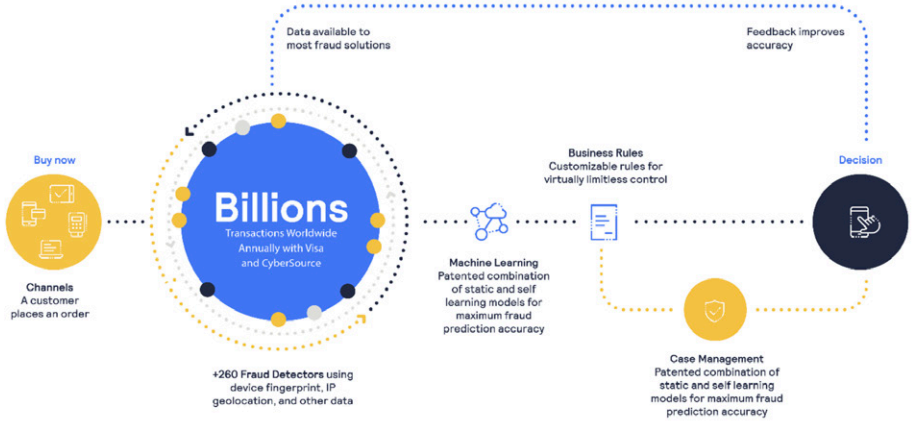
The combination of machine-learning results and rules is possible with this system. For example, a merchant can create a rule that takes a score threshold and uses it alongside other order attributes (for example, if the score is greater than 80, and the billing address doesn't equal the shipping address).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

The **Rules Suggestion Engine** is a feature in Decision Manager that 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 Decision Manager Replay, which can help confirm the future value of a rule or rule set.

**Decision Manager Replay** is another feature in Decision Manager that allows merchants to test and 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.

**Identity Behavior Analysis** is the latest enhancement to Decision Manager that works in the background to help recognize good customer behaviors using positive info codes. It can increase the acceptance rates for future transactions. This is a value-added service in Decision Manager and no additional cost to the merchant. It is another tool in the DM toolbox similar to DM Replay and Rules Suggestion Engine. It provides a competitive advantage by focusing on the positive instead of the negative transactions to capture more revenue. It recognizes both positive and negative customer behavior usage over time using elements like account number, email, etc. to track and flag consumer behavioral changes within merchant data and across merchants. The real-time machine-learning analysis provides new Decision Manager info codes for both positive and negative behaviors to help increase acceptance rates and detect fraud more effectively. It can easily detect new customers using these behavior codes.

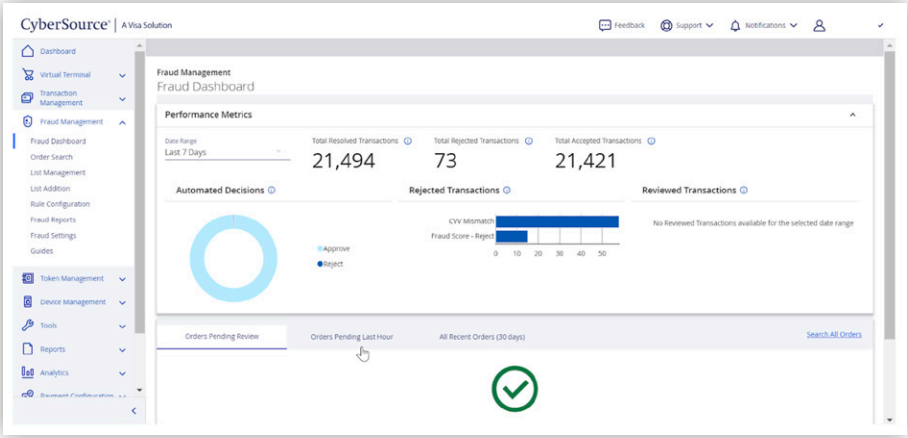



Pre-authorization transaction screening through Decision Manager runs Decision Manager prior to authorization, resulting in a "cleaner" set of transactions sent to the issuer for evaluation. Over time, the issuer would analyze, recognize, and establish that a lower rate of declines (active involvement)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

Merchants can also integrate Payer Authentication in Decision Manager as a full component platform service. Enhancing the integration for Payer Authentication (CardinalCommerce) as a full component service allows Decision Manager 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 3-D Secure benefits to merchants without compromising the customer experience.

**Cybersource's Account Takeover Protection** defends online accounts from unauthorized access. It includes a flexible rules engine that allow businesses to identify suspicious activity based on behavior, email, device, communications, and other predictive attributes. This service helps to identify and block account takeovers, fake account creations, loyalty fraud, and other pre-transaction attacks. It can be used as a stand-alone service, or can be integrated with Decision Manager, adding an extra layer of sophistication by allowing users to leverage learnings between account activities and payment transactions.

**Cybersource** offers a chargeback guarantee product (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.




In 2020, Cybersource introduced Fraud Management Essentials, a lightweight yet robust and flexible fraud management solution. It is a streamlined fraud management solution that benefits from the scale, security, and analytics of Visa and Cybersource, enabling growth from micro to enterprise on a single platform.

Fraud Management Essentials helps businesses minimize common fraud attacks. With ready-to-go fraud filters, merchants can

automatically monitor orders and provide a seamless customer experience. The service leverages Decision Manager's powerful computer models using machine learning and hundreds of validation tests to prevent fraudulent transactions. Users can accelerate setup with built-in fraud rules and then make informed decisions via a user-friendly dashboard. Users can take advantage of the automation of machine learning while retaining control over risk tolerance. And they can do so while reducing chargeback and declined authorization costs of card testing and common fraud attacks.

## 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. With deep insights across industries and geographies, plus performance monitoring tools, Managed Risk Services provides enrolled businesses with a dedicated risk analyst to maintain their fraud strategies as well as customized insights. A risk analyst monitors the fraud prevention strategy of the business and applies real-time adjustments based on the objectives of the business. Because they operate across our entire client base, they can identify fraud patterns before a business would see a fraud trend developing in their data.

# Cybersource



In addition, the **Cybersource** Global Screening Management team can manually review orders on clients' behalf in conjunction with risk analysts to manage their fraud operations.

**Cybersource** offers different levels of service to support your business needs.

- 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, which 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

**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.

Additionally, Visa recently acquired Verifi, a leader in technology solutions that offers dispute resolution capabilities. Verifi's products and services will be made available through **Cybersource** in the future.

# Kount



**Kount** joined Equifax in early 2021. Combined, Equifax and **Kount** power digital risk assessment, helping businesses establish greater Identity Trust behind each consumer interaction. With **Kount**, Equifax expands the company's worldwide footprint in digital identity and fraud prevention solutions. Global businesses can harness the power of AI better than ever before to establish strong digital identity trust—and engage better with their customers online.

**Kount's Identity Trust Global Network™** delivers real-time fraud prevention and account protection. It enables customer experiences for more than 9,000 brands and works with over 50 payment processors and card networks. Linked by Kount's award-winning AI, the Identity Trust Global Network analyzes signals from 32 billion annual interactions to personalize user experiences across the spectrum of trust—from frictionless experiences to fraud blocking. Their Identity trust decisions focus on delivering safe payments, account creation, and login events while reducing digital fraud, chargebacks, false positives, and manual reviews.

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

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

Kount®

## At a Glance:

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

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

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

## Products

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

- **Kount Command™** for payments fraud protection
- **Kount Control™** for account takeover protection
- **Data on Demand,** fueled by Snowflake, for actionable customer insights
- **Near Real-Time Chargeback Prevention,** integrated with Verifi, A Visa Solution, for managing fraudulent transactions, chargebacks, and disputes

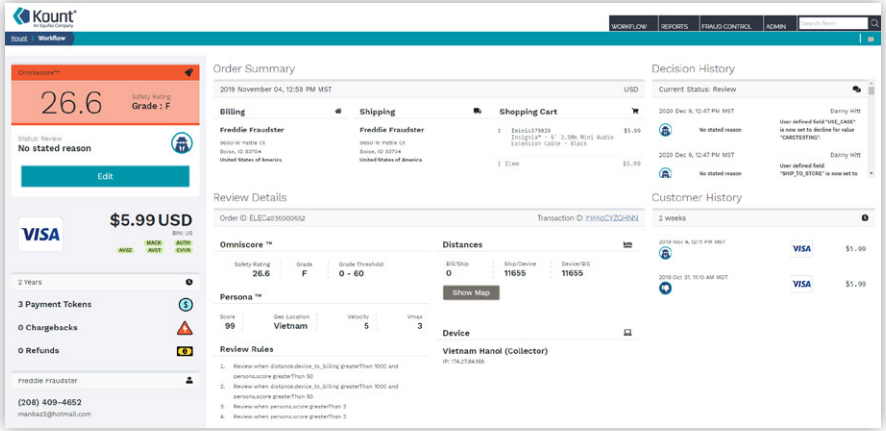
**Kount Command** protects thousands of leading brands globally, including online merchants, digital businesses, and enterprise-level retailers against digital payments fraud. **Kount Command** also helps businesses reach and maintain desired business outcomes around chargebacks, approval rates, manual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

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

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

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

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




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

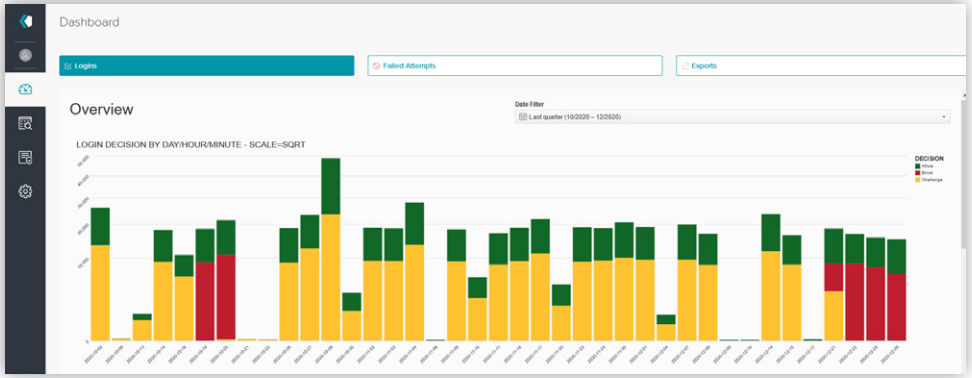
In the protection layer, **Kount Control** evaluates user behavior and device and network anomalies to detect high-risk activity such as bots, credential stuffing, and brute-force attacks. Kount then determines, in real time, whether to allow a login, decline it, or challenge it with step-up authentication.

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

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

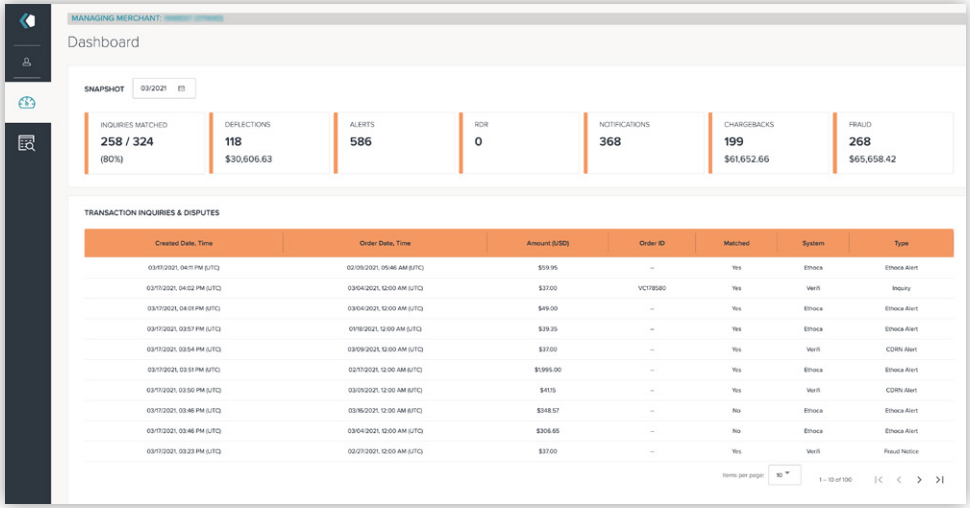
# Kount






**Kount's Data on Demand** offers insights to improve customer experiences, reduce friction, increase conversions, and uncover cross-sell and up-sell opportunities. It enhances a company's customer knowledge with thousands of additional data points from the **Identity Trust Global Network**. Combining data from multiple sources can help businesses analyze purchase and product usage behaviors to personalize marketing campaigns, products, and services to customers. This knowledge can also help identify more up-sell and cross-sell opportunities. It can also help businesses approve more good orders and improve fraud prevention strategies. Businesses can analyze the data on its own or combine it with additional company-collected data for deep analytics on one platform. Data on Demand was built on Snowflake and is hosted by **Kount** in a private data warehouse.

**Near Real-Time Chargeback Prevention** is a solution that can provide chargeback mitigation and help manage disputes. **Kount** has integrated with Verifi, A Visa Solution, to launch the chargeback prevention solution in 2020. Customers can take advantage of chargeback prevention tools to identify, prevent, and resolve chargebacks without the need for development resources or complex integrations. **Near Real-Time Chargeback Prevention** delivers all of the benefits of **Kount's** fraud prevention and enhanced capabilities of Verifi's dispute management tools to help stop chargeback losses and reduce dispute timeframes.



## Partners

Customers can gain access to the Identity Trust Global Network and **Kount's** solutions by working with **Kount** directly or via **Kount's** partner network. Kount has partnerships with more than 50 payment service providers, gateways, and partners globally, including J.P. Morgan Chase, Barclays, Moneris, Braintree, BlueSnap, and others. **Kount** also partners with ecommerce platforms and payment partners, such as Magento, Shopify, and FreedomPay among others.

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

## Features and Functionality

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

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

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

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

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

**Email Insights** uses identity trust data to determine an email address' date first seen and date last seen. Knowing the age of an email address can trigger additional friction if needed to authenticate the identity behind the transaction and help prevent fraud. Further, **Email Insights** helps businesses understand if an email address has been associated with criminal fraud, friendly fraud, or risk.

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

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

## Professional Services

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

**Kount's Chargeback Guarantee** allows customers to stabilize their fraud expenditures with predictable costs and guaranteed protection against criminal fraud, chargebacks, and losses. The **Chargeback Guarantee** provides instant approve/decline decisioning with 100% coverage of eligible fraud-related chargebacks.

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

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

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

# Kount



**Kount's** experienced fraud experts and hand over fraud prevention decisioning.

**Kount's Consulting Services** provides access to a broad team of fraud professionals with expertise across multiple industries and specialties. Businesses gain training for fraud analysts on manual review best practices, progress reporting, and expert guidance regarding control measures to implement throughout the customer journey.

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

**Sift** is focused on digital trust and safety, empowering businesses of all sizes to protect themselves from fraud and abuse while growing revenue. Some of the largest merchants in the world—including Twitter, Airbnb, and Wayfair—trust **Sift** to help deliver positive customer experiences while preventing fraud and abuse. 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.

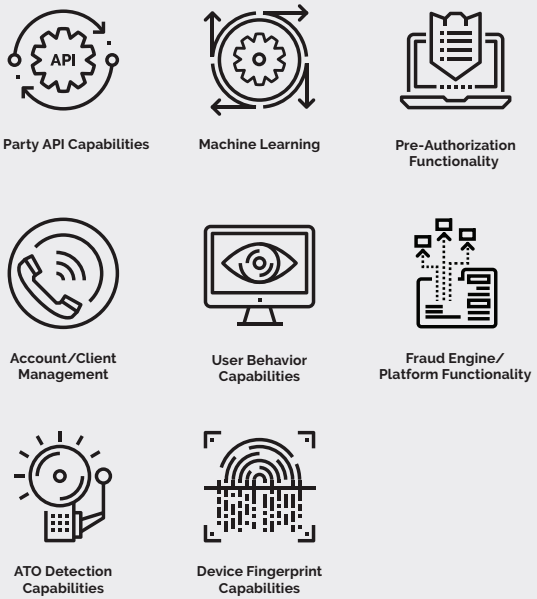
## Solutions & Functionality

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 the user journey, **Sift** is able to detect multiple types of fraud (payment fraud, fraudulent content, account takeover, promotion abuse, and fake accounts) and provide a risk assessment of how trustworthy an interaction is.

**Sift** combines global models with custom learning and extensive feature engineering to deliver accuracy and enable dynamic, real-time decisioning. The global models anonymously share insights about new, emerging fraud patterns across the network,

### At a Glance:



boosting prediction accuracy by up to 30 percent. These are blended with custom 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, enabling instant action—from automatically blocking or accepting users to dynamically tailoring the level of friction in 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 by ingesting it via APIs or using **Sift's** customizable web-based console. The console gives trust and safety teams of all sizes a tool to investigate fraud patterns, automate decisions, do manual review, 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 accessible through the web-based console. Products include:

Payment Protection

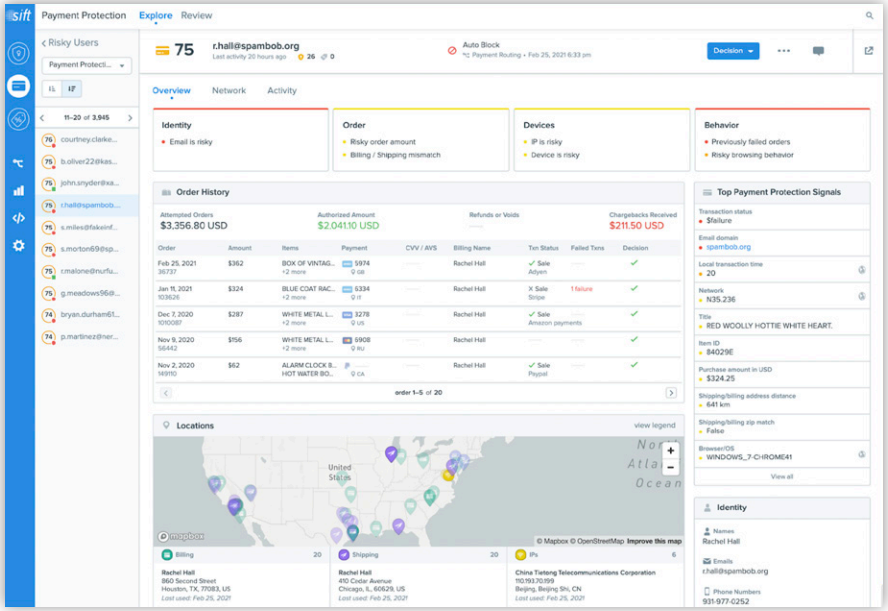
- Proactively stop fraudulent chargebacks and protect revenue
- Block fake accounts and risky signups
- Streamline operations and reduce manual review
- Grow revenue with decreased false positives and increased conversion

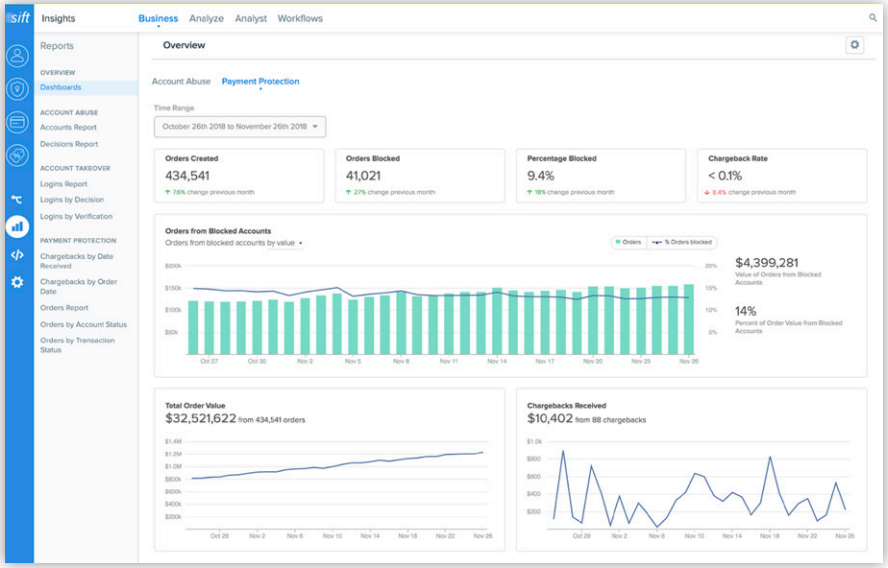
Account Defense

- Stop account takeover attempts to secure user accounts and stored value
- Apply multi-actor authentication (MFA) to authenticate risky sessions
- Reduce friction for trustworthy sessions

Content Integrity

- Reduce fraudulent content like spam and scams
- Block fake accounts and risky signups
- Safeguard your brand and create better user experiences
- Work efficiently and reduce manual moderation



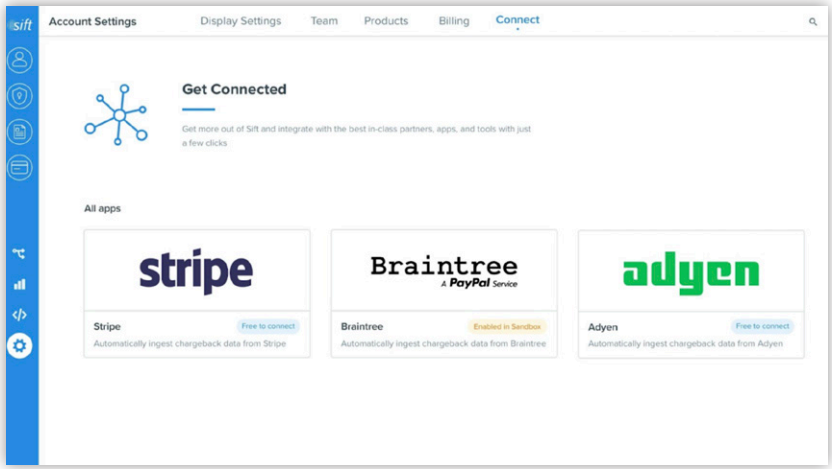

All of **Sift's** products are accessible via a single web-based console. The console's capabilities include:

- **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 any signals shared with other users.
- **Manual review queues:** Customers can queue users, orders, or content for manual review based on customizable criteria that leverages the **Sift** Score and other fraud signals. Queues automatically assign open cases to individual analysts while avoiding overlapping reviews. They also support escalation and hold functionalities for additional review by senior analysts or managers.
- **Automated Workflows:** Trust and safety teams can automate decisions and business processes by defining automated workflows based on customizable criteria using "if/then" analysis. Workflows are completely customizable and can be, for example, configured to automatically reject risky users, reduce friction for trusted users, assign transactions to analysts for manual review, and initiate additional verification processes such as 3D Secure and SMS verification.

- **Customizable roles and permissions: Sift** supports multiple user types with a wide range of permissions depending on the requirements of their role. For example, admins may have access to manage workflows, analysts may have access to order details and the ability to make decisions, and a developer may only have access to integration health information. Customers can configure custom permissions to suit their team needs.
- **Multilevel account support:** Customers can set up sub-accounts within a global account to support multiple business units, geographic regions, etc. Sub-accounts are easy to jump between, and a global view provides aggregated insights across all sub-accounts.
- **Real-time analytics:** Admins can track business health with comprehensive insights that report on order block and accept rates, chargeback rates, risky signups, 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 Connect** makes **Sift** the hub for trust and safety teams, pulling together the data and tools required to operate efficiently in one place. Using apps and open APIs, customers are able to integrate faster, improve accuracy and efficiency, and drive action across their organizations.

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



## 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 strategy. Support engineers are also available to answer any questions about product usage and technical details. Integration, account management, regular support, and trust and safety assessments are all included. Premium support plans can be purchased based on volume and need.

## In development in the next 6-12 months

- Score analysis and automation testing for enhanced accuracy and more confident operations.
- Pipelines with leading cloud data warehouses to enable deep analysis and transparency across teams.
- An expanded ecosystem of integrations with technology partners and white-glove service providers for more tailored solutions.

# Signifyd



**Signifyd** provides an end-to-end Commerce Protection Platform that leverages its Commerce Network to maximize conversion, automate customer experience, and eliminate fraud and abuse for retailers.

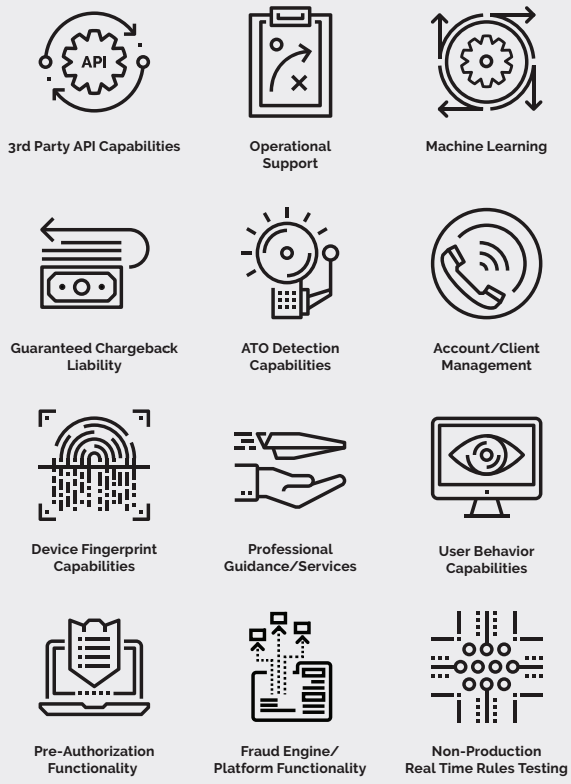
**Signifyd** uses big data, machine learning, and expert manual review to provide a 100 percent financial guarantee against fraud and abuse on approved orders that turn out to be fraudulent. This effectively shifts the liability for fraud away from ecommerce merchants, allowing them to increase sales and expand into new markets while reducing risk.

Among its customers, **Signifyd** counts a number of companies on the Fortune 1000 and Internet Retailer Top 500 lists. **Signifyd** is headquartered in San Jose, CA, with locations in Denver, New York, Belfast, London, and Mexico.

**Signifyd** helps merchants overcome key challenges by:

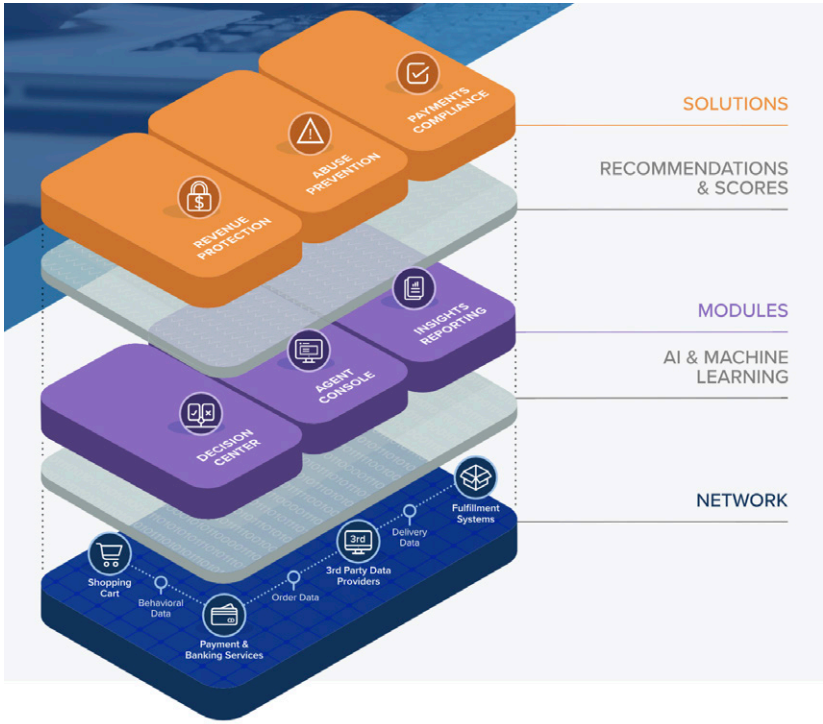
- **Reducing friction in the customer experience:** Today's consumers expect more from their shopping experience than ever before. Friction is not tolerated, and as merchants begin to compete on their customer experience, a fast and secure checkout, real-time updates on order progress, and avoidance of step-up authentications become crucial.
- **Promoting revenue optimization:** At every stage of the conversion funnel, there are 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, lost revenue from 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

## At a Glance:



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 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

The **Signifyd Commerce Network** is the foundational powerhouse of the Commerce Protection Platform. The network includes thousands of merchants selling in more than 100 countries supporting more than 250 million consumers. It's the source of a huge amount of transactional and behavioral data that gives **Signifyd** a full and deep picture of commerce across the globe. The vast amount of data and transactions means that 98% of transactions made today are made by consumers that **Signifyd** has seen before.

**Signifyd's** Commerce Protection Platform maximizes conversion, automates customer experience, and eliminates fraud and abuse. The platform is made up of three distinct solutions.

### Revenue Protection

Provides a complete financial guarantee on all approved orders. The solution's Overflow Protection automates order flow effortlessly and scales up endlessly through seasonal peaks. By shifting liability, merchants can open up the conversion funnel with confidence by relaxing restrictive rules put in place by banks and payment processors' authorization solutions and rules.

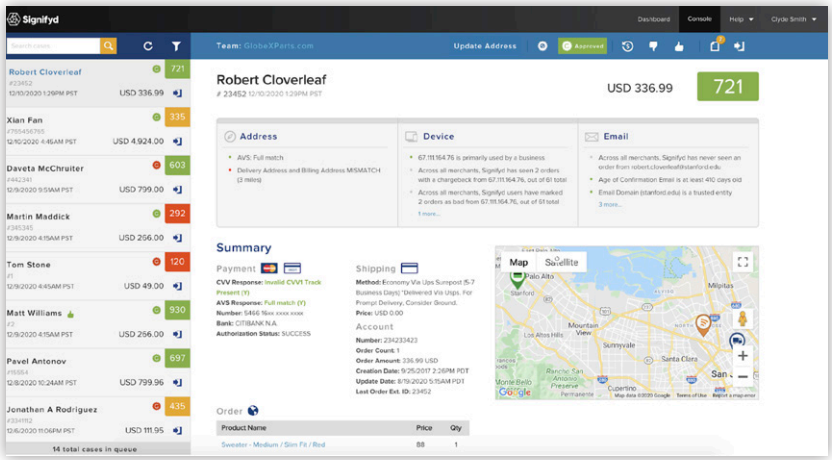
### Abuse Prevention

Merchants are protected from unwanted policy abuse and

provided a complete financial guarantee on abusive INR chargebacks. Intelligent Order Triage and automated Chargeback Recovery services ensure merchants can effectively manage post-purchase customer experience costs. The solution relies on the same intelligence that **Signifyd** uses to protect merchants from fraud. Abuse Prevention allows merchants to address all forms of chargebacks, not just fraud chargebacks.

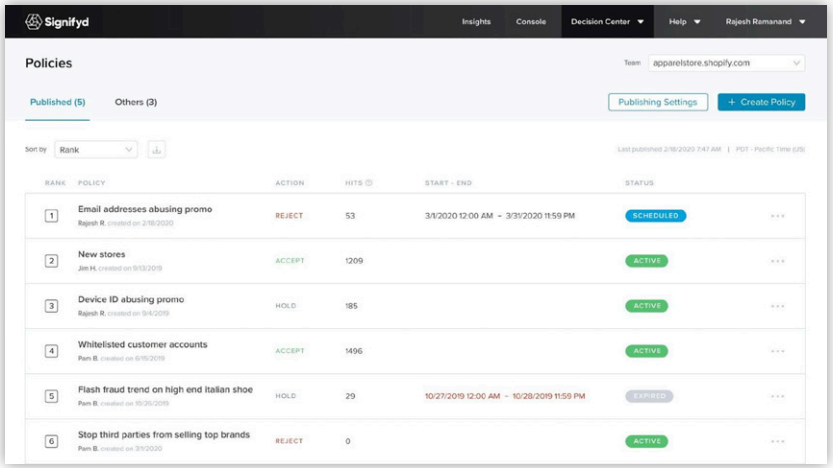
### Payment Compliance

Payment Compliance gives **Signifyd** merchants a frictionless and future-proof authentication experience, including PSD2 compliance, OFAC checks, etc. **Signifyd** manages compliance issues so merchants can focus on serving customers. The Payment Compliance solution incorporates a number of features to stem revenue leakage.



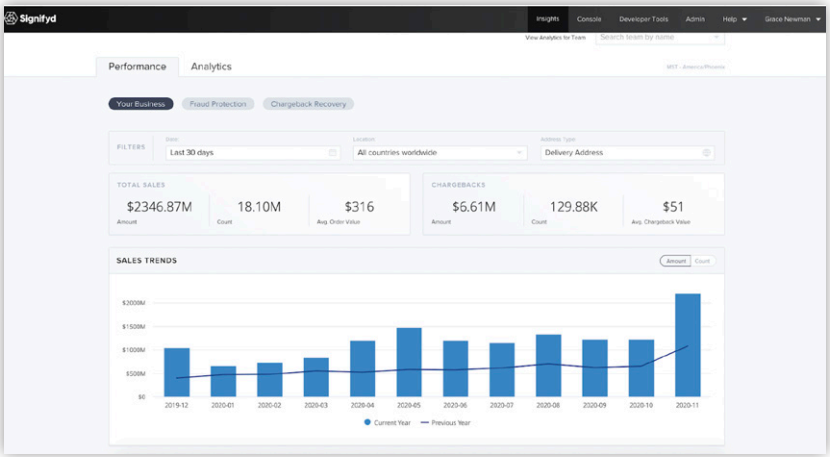

The Commerce Protection Platform comprises three core modules.

**Agent Console** provides a single view of all transaction information and offers operations and payments teams full transparency on every order and decision. **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 decisions.




**Decision Center** provides the complete set of tools risk analysts need to analyze, identify, and control abusive scenarios. **Decision Center** exposes the same data points–like device information, email data, and network intelligence–their fraud detection models have utilized for years. Merchants can use this library of hundreds

of data points to easily create and manage custom business policies via an intuitive user interface. With **Decision Center**, merchants can test and simulate new policies before go-live to ensure loyal customers are never negatively affected and abusive scenarios are managed as intended.




**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.

## 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, Shopify, and Shopify Plus+.

## 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.

# 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.

Apruvd.

## 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:


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

# Experian



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

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

**FraudNet** is comprised of four core components:

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

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

## At a Glance:


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

# Feedzai



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

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

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

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

## At a Glance:

Machine Learning

Fraud Engine/ Platform Functionality

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

# IdentityMind



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

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

## At a Glance:

Machine Learning

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

# NoFraud



**NoFraud** is a full-service fraud prevention solution offering automated ecommerce fraud prevention through real-time virtual identity verification. They deliver individual, real-time decisions for each transaction using thousands of data points and virtually every fraud detection technology available. **NoFraud** focuses on eliminating all fraud-related overhead and required expertise from its customers. They increase customers' approval rates and eliminate their chargeback liability through a combination of machine-learning technology and human intelligence.

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

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

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

NOFRAUD

## At a Glance:


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

# NoFraud



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

# Radial



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

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

Benefits include:

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

Radial

## At a Glance:


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

# 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.

# SEON



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

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

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

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

## At a Glance:


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

# Simility



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

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

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

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

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

## At a Glance:

Machine Learning

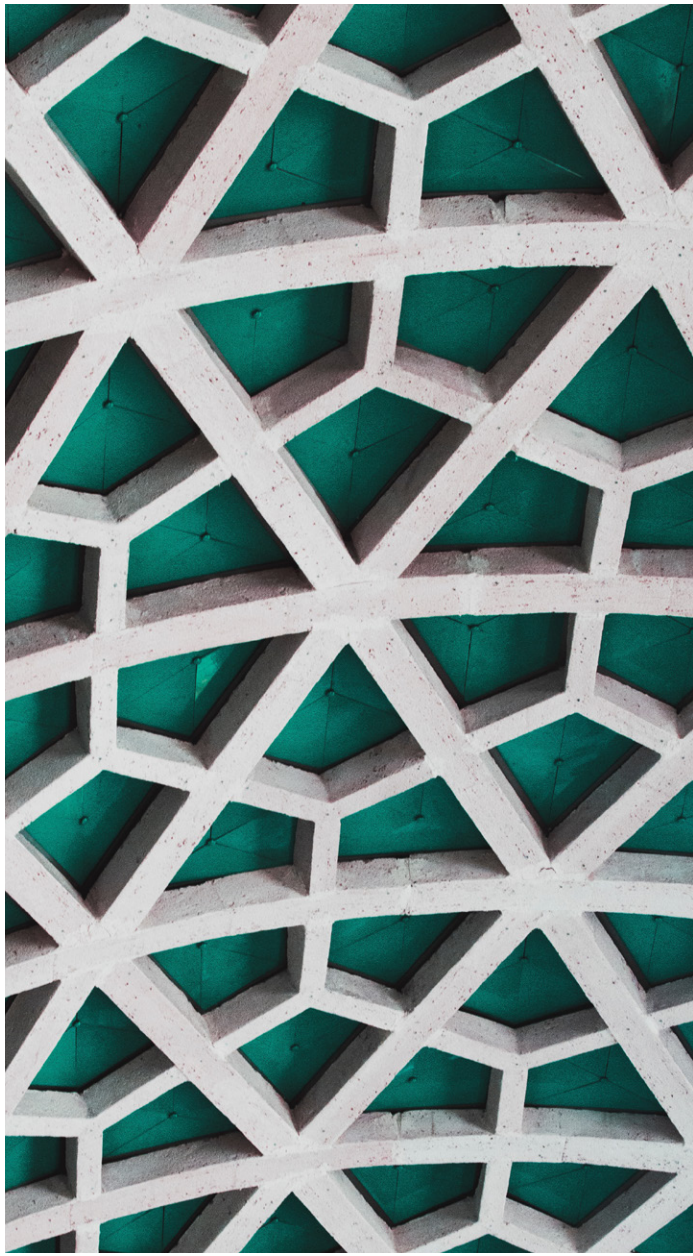
Fraud Engine/ Platform Functionality

Device Fingerprint Capabilities

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

# Identification & Data Verification

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



# ArkOwl



**ArkOwl** is a real-time data provider offering email address and phone number verification. Using only an email address and a phone number, they provide 83 unique data points to help identify fraudulent patterns and activity. This functionality can help minimize fraudulent attempts while maximizing ability to identify legitimate users. They process over 14,000,000 transactions annually.

Available data is 100 percent live in real-time. No data is pulled from stale, potentially outdated databases. Privacy is taken seriously with all data requests anonymized as requested through **ArkOwl**, so various providers of the data points seen in **ArkOwl** cannot track information on customers. To keep customer data absolutely private, they do not store any in the first place. Because the data is aggregated and presented in real time, there is no need to depend on storing and sharing data from customers. In addition, all connections are secured with 256-bit encryption.

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

## At a Glance:


3rd Party API Capabilities

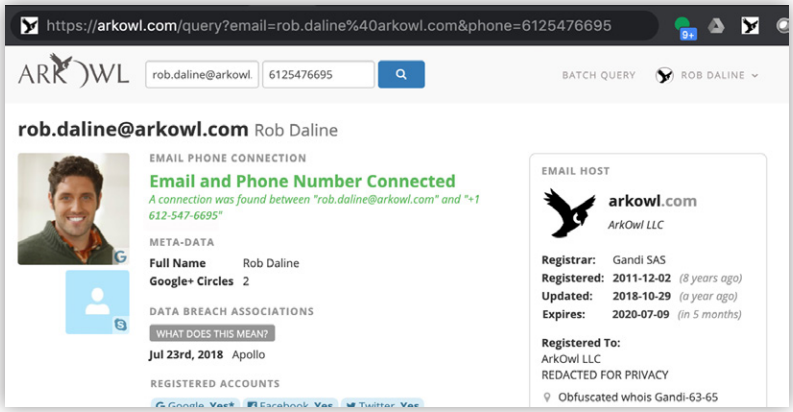
Professional Guidance/Services

Pre-Authorization Functionality

# ArkOwl



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




**Reporting:**

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

**Service / Support:**

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

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

**Users and Pricing:**

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

**Integration:**

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

A manager account is created for user management purposes.

# ArkOwl



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

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

**Near-future road map:**

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

# EKATA



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

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

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

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

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

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

## At a Glance:


3rd Party API Capabilities

Machine Learning

Pre-Authorization Functionality

# EKATA



With over 20 years of data sourcing experience and strong global presence, Ekata helps over 2,000 companies verify trusted identities while fighting fraud in industries including ecommerce, financial services, payments, and marketplaces.

## Data Profile

The Identity Engine data provides unique and predictive insights for five key identity attributes: name, phone, email, address, and IP, that can be categorized as the following:

- **Identity elements**
  Clean identity data that has been parsed, normalized, and deduplicated
- **Match statuses**
  Status that indicates whether an identity element is a match to the name provided within the query such as a phone to name match (one exception to this is an additional phone to address match)
- **Validity checks**
  Validity of an identity element, and in some cases, validity down to a specific level (for example, street, unit number)
- **Distance calculations**
  Distance (in miles) between two identity elements such as an IP address and physical address
- **Enriched metadata**
  Metadata that provides deeper insight into an identity element (for example,ex. phone line type, address geocoordinates, etc.)
- **Risk flags/score**
  Proven, machine-learning model-derived predictions to help assess the risk of a particular attribute, combination of attributes, or a digital identity as a whole
- **Network signals**
  Derived from real-world usage of elements, these signals add up to transaction-level intelligence; it's clear how an identity element has been previously used (for example, how many transactions an element was seen being used in, how many merchants an element was used at, etc.)

**Security and 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. With billions of data points provided by our 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.

## Products

### Identity verification suite

**Transaction Risk API**

The Transaction Risk API maximizes approval rates while fighting payment fraud in every transaction. In under 100ms, it delivers a concise response to expedite authorizations and reduce customer friction.

The Transaction Risk API provides critical insights to help detect transaction fraud using the following:

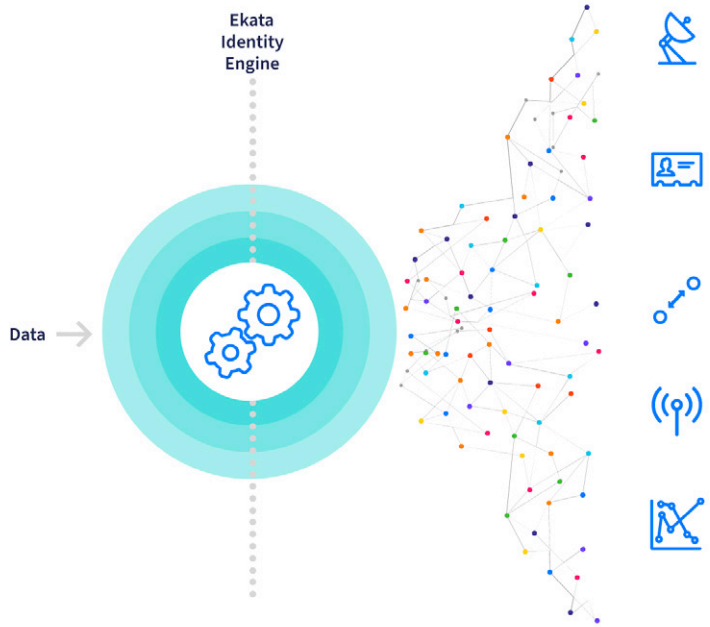
Validity checks for payment details such as primary and secondary email, phone, and address provided by the customer

Match statuses to confirm that the primary and secondary email, phone, and addresses provided in the transaction are associated with the customer

IP distance from address calculations to gauge the distance between a provided IP and address

Risk flags and scores to assess the risk of the holistic digital identity (Identity Risk Score), previous usage of identity elements (Identity Network Score), and the risk of a provided IP (IP Risk Flag)

Enriched phone metadata to gain insight into the line type of the phone number




**Account Opening API**

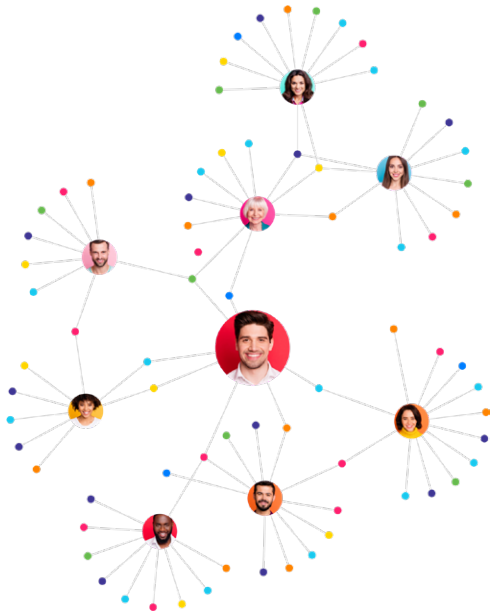
The Account Opening API identifies potential bad actors from good customers during the online application process. It is designed to expedite the user experience for good customers while preventing

bad actors from using stolen or synthetic identities to gain instant credit, seek loans, launder money, or carry out credit bust-out schemes.

Attracting, onboarding, and converting customers in the evolving transformation of digital and traditional banking requires the ability to confidently identify customers. The Account Opening API can improve account opening and onboarding workflow experience by helping to verify digital identities to increase conversions, prevent fraudulent account creation and reduce customer friction.

The Account Opening API provides critical insights to help detect sign-up fraud using the following:

- Proprietary Network signals to assess the riskiness of the location address (IP last seen), the phone (phone last seen), and the combination of the phone and email provided (phone email first seen)
- Match statuses to confirm that the email, phone, and address information provided in the application are associated with the customer name
- Enriched phone metadata to gain insight into the line type of the phone number, the phone carrier, and country code
- IP distance from address calculations to gauge the distance between a customer's IP and their provided addresses
- Risk flags and scores to assess the risk of the holistic digital identity (Identity Risk Score), previous usage of identity elements (Identity Network Score), and the risk of a provided IP (IP Risk Flag)



**Pro Insight for Manual Review**

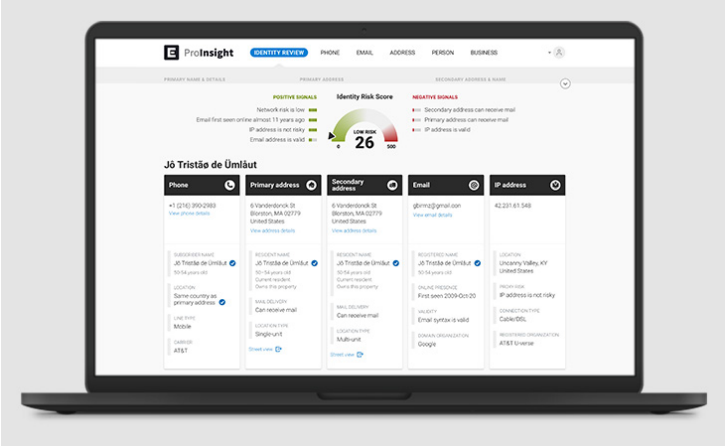
Pro Insight provides tools designed to assist users in improved decision making. It offers a summary of the key data immediately upon access, and the ability to dive deeper into specific data points to gain clarity and increase decision accuracy.

Pro Insight provides insights to help manual review agents assess the risk of any transaction using the following:

# EKATA



- An in-depth look inside how the Identity Risk Score was generated with positive and negative risk indicators
- Distance calculations between various inputs such as IP and shipping and/or billing address
- Signals from the Ekata Identity Network to provide insight into how a customer-provided identity elements are being used online (for example, primary address and IP first seen together a month ago)
- Reporting and analytics on usage, users, and coverage




## Identity element risk suite

**Address Risk API -**

The Address Risk API validates global addresses and provides fraud risk signals in fractions of a second for customers to streamline checkouts, identify fraud early in customer workflows, and enforce business policies.

The Address Risk API provides critical insights to help identify whether an address is high or low risk using the following:

- Unique identifiers for any address that can be used to perform velocity calculations
- Validity check of an address, down to a specific level (i.e., street, unit number, etc.)
- Normalized addresses to consistently format addresses
- Geo coordinates for calculating distances from other reference points as part of risk analysis to establish geographic risk "zones"
- Network signals to provide real world, transaction-level intelligence into how an address has been used online (for example, if an address was used in 10 transactions in the last 90 days)

**Phone Intelligence API**

The Phone Intelligence API verifies the risk of a customer with phone metadata and associated locations, personas, and businesses.

The Phone Intelligence API provides intelligence for risk analysis using the following:

- Carrier information to identify the company that provides voices and/or data services
- Validity check of a phone number
- Country details with access to the country calling code, country code, and country name associated

- Prepaid account check to understand whether the phone number is associated with a prepaid account
- Unique identifier that can be used to perform velocity calculations

## Integrations and Additional Services Offered

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

**Pro Insight Integrations**

- **Hyperlinks through existing partnerships:** Generally, merchants can activate a hyperlink in their existing fraud platform to access **Pro Insight** manual review solution with a single click. Existing partnerships include **Accertify**, **CyberSource**, **Experian**, and **Kount**.
- **Custom hyperlinks:** These 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 provide 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.

## API Integrations

Direct platform partnerships: Ekata 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 Ekata 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.

# Emailage



**Emailage**, founded in 2012 in Chandler, Arizona, is a global risk management and fraud detection technology company. They help businesses deter online fraud and aid in the delivery of low-friction customer experiences through key partnerships, proprietary data, and machine-learning technology.

**Emailage's** Intelligent Fraud Detection and Risk Decisioning Solutions build a multifaceted profile associated with a customer's email address and renders predictive scoring for email risk, digital identity, and risk decisioning confidence. **Emailage** solutions are available through direct integration as well as partner channels. **Emailage** partners include Accertify, CyberSource, Equifax, Experian, and LexisNexis Risk Solutions.

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

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

emailage™
GLOBAL FRAUD PREVENTION

## At a Glance:


3rd Party API Capabilities

Account/Client Management

Machine Learning

Professional Guidance/Services

# Emailage



## Solutions & Functionality

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

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

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

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

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

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

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

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

# Emailage



- Technology
- Gaming
- Event ticketing
- Lending

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

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

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


**Reporting and UI**

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

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

# Emailage



## Services Offered

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

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

## Integration Options

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

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

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

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

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

# Emailage



## Pricing

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

# GeoComply



**GeoComply** provides a reliable and accurate geolocation solution for fraud detection.

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

With technology proven and refined over 10 years of development and billions of transactions, **GeoComply** can accurately determine a users' true location and whether they are attempting to mask their location using various spoofing tools.

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

**GeoComply** enables a wide range of industries including banks, fintechs, and cryptocurrency exchanges to detect and guard against geolocation-based fraud.

GEOCOMPLY
Empowering The Future Of Digital Trust

## At a Glance:


## Four typical use cases for GeoComply:

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

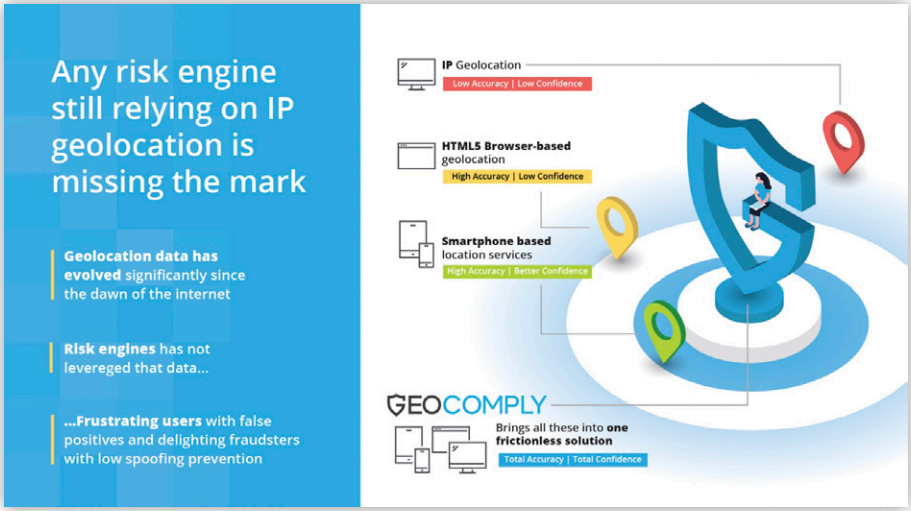
- **AML and Sanctions Compliance** - Ensure compliance with jurisdictional requirements by verifying the true location of a transaction.
- **Authentication and Account Protection** - Monitor account updates and user behaviour by adding geolocation checks to continuous authentication and protect against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

## Some of the key benefits from GeoComply:

- **Strengthen KYC and CDD** - "Spoof-proof" and accurate geolocation data (beyond a simple IP address) is a crucial component of AML and CFT processes by ensuring that KYC due diligence is robust and protected from exploitation.
- **Fraud Prevention and Risk Mitigation** - Real-time and historic analysis of geolocation transactions strengthens risk management by creating a holistic oversight of user behavior. Suspicious activity can be prevented in real-time and identified over time.
- **Reporting and Traceability** - All geolocation transactions are maintained in a secure database and archive, creating audit trail transparency and traceability. This strengthens reporting capabilities of FIs for regulators and law enforcement.
- **Sanctions Compliance** - Compliance-grade geofencing capabilities add extensive location assurance through the collection of multiple and unaltered geolocation data sources, which strengthens sanctions compliance. IP-based solutions do not constitute location due diligence.

## Products and Services

**GeoComply** represents considerable advancement in fraud detection as it relates to historically available geolocation and location-based signals. While direct competition for **GeoComply** is limited, they do consider they are competing against the notion that an IP address is sufficient for location-based risk management.



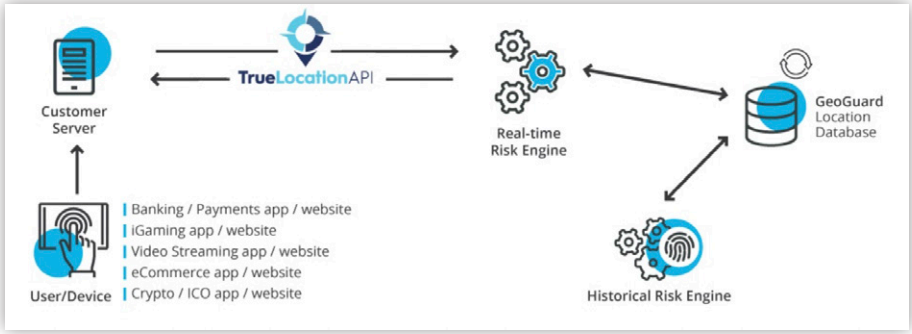

In addition to geolocation, **GeoComply** uses a proprietary device fingerprinting technique to enhance its fraud detection capabilities. Traffic filtering and flexible rules can be configured to meet specific business needs.

# GeoComply

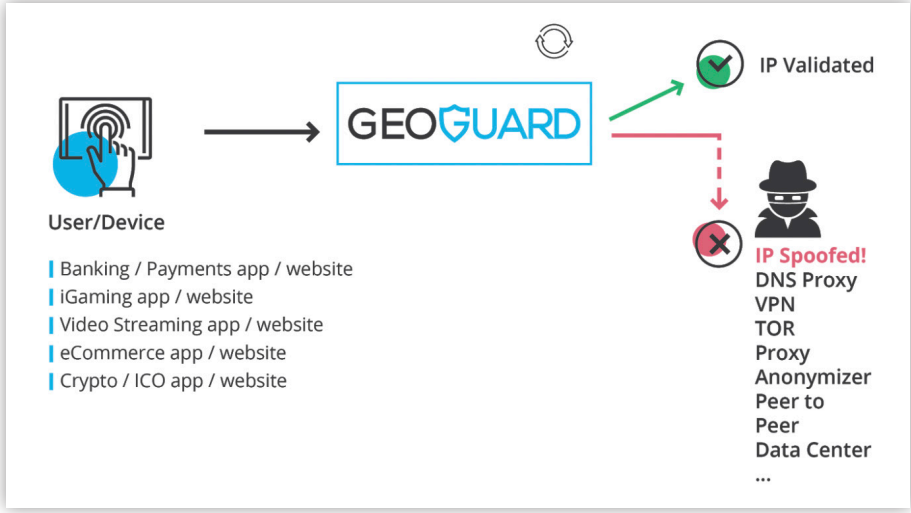


**GeoComply** Mobile and Desktop SDKs represent a high standard in geolocation security for risk and compliance management, ensuring continued high performance and accuracy for location compliance. It is embedded in native mobile apps or desktop applications, providing geolocation identification during a user's session.

**GeoComply** offers a geolocation solution that works directly within the client's website for all devices and user interfaces. For frictionless and spoof-proof geolocation within the browser, this geolocation experience can be customized according to the business and compliance needs of the client, with adaptable end-user prompts and secure collection of location data.




**TrueLocation API** provides location-based fraud detection, utilizing both a real-time risk engine and a historical risk engine to identify and flag potentially fraudulent activity. By analyzing both real-time and historical data, TrueLocation API enables organizations to identify and stop a wide variety of fraud including chargeback fraud, account sharing, card not present (CNP) fraud, account takeovers, and detecting VPN usage.




**GeoGuard** provides multilayered fraud protection against VPNs, proxies, peer-to-peer networks, and other types of IP data manipulation. Their solution is continuously updated as new threats and data centers are identified and mitigation methods are developed.

**GeoComply** achieves advanced and accurate geolocation security through three key steps:

1. **Step 1- Collect data:** Collect geolocation data from multiple sources, including: GPS, WiFi, GSM, Browser/HTML5, and IP address.

2. **Step 2 - Ensure accuracy:** Validate data points are trustworthy by ensuring they are:
   - Not being altered via spoofing apps,
   - Accurate, by combining multiple location signals in the location algorithm, and
   - Physically there by monitoring for remote access apps/ signals.
3. **Step 3 - Analyse behavior:** Conduct real-time and historical analysis on the collected dataset to detect and flag likely patterns of location fraud. **GeoComply** uses both machine learning and human intelligence with dedicated fraud and data analyst teams.

Additionally, **GeoComply** has a KYC solution focused on regulated markets:

- **IDComply** allows businesses to query multiple vendors for both ID and age verification, allowing banks, payment processors, and other transaction-based businesses to move from a single vendor of ID and age verification to a multi-vendor model, through one API call. By integrating IDComply into user onboarding processes, companies working in multiple jurisdictions can also manage the patchwork of compliance requirements – not only for age and ID verification but also anti-money laundering (AML), know your client (KYC), enhanced due diligence (EDD), PEP/Sanctions Watch List/Adverse Media, child support, and other requirements.

## Reporting and Analytics

Most users consume **GeoComply's** ingested signals from within their existing tools, **GeoComply** also provides a single portal with a wide range of out-of-the-box reporting and dashboards.

Users can access detailed logs and information about each transaction through real-time monitoring or with after-the-fact drill-down reporting. Examples of reports include but are not limited to:

- Transaction level reports (archived for 7+ years)
- Visualization of user location with Pin Drop Maps
- Detailed device attributes to support incident review
- Users per IP address and device, and IP addresses and device per user
- Reasons for inability to pass the geolocation check
- Chargeback Report shows the location and device used for all of a client's transactions within a certain timeframe.

Analytical insights are available through GeoComply's client Kibana analytics tool, which contains dashboards and custom reporting for detailed analysis of potentially fraudulent transactions. Additional real-time data is also provided via RESTful APIs.

## Integration process

**GeoComply** has a well-established implementation process, with fully supported integration and launch phases. The company works closely with each client to map the entire user experience and identify where the use of location data can reduce fraud. A comprehensive white-glove onboarding process covers everything from integration design through certification and launch support. The integration process also includes a set of onboarding support hours.

## Level of support

Standardized ongoing support is also available and meets SLA commitments. Organizations are assigned a primary point of contact who provides weekly catch-up sessions to address any issues and provide a "health check," calling out potential issues before they happen, as well as round-the-clock contact numbers for urgent issues.

**GeoComply's pricing model is based on:**

- Tiered pricing by transaction volume
- A monthly minimum fee

**Key developments on the calendar for the next 12 months:**

- Use TrueLocation API for clients capturing their own in-app geolocation information
- Focus on partnerships with complementary platforms to integrate with your existing tool stack and enhance your team's incident review and reporting flows.

# Intent IQ



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

Verticals utilizing their products and services include ecommerce, financial institutions, and the media ecosystem. **Intent IQ** products and technology are backed by over 150 granted patents. Vectors of focus include account takeover and new account fraud.

For ecommerce and financial institutions, **Intent IQ** validates a device user's claimed identity credentials. It checks whether the given device matches the devices of the claimed identity home by comparing different parameters that are difficult to mimic. The home is located by **Intent IQ** using the claimed identity postal address converted to latitude/longitude and claimed email.

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

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

## At a Glance:


3rd Party API Capabilities

Professional Guidance/Services

Pre-Authorization Functionality

ATO Detection Capabilities

# Intent IQ



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

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

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

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

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

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

The file includes the following requested data fields:

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

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

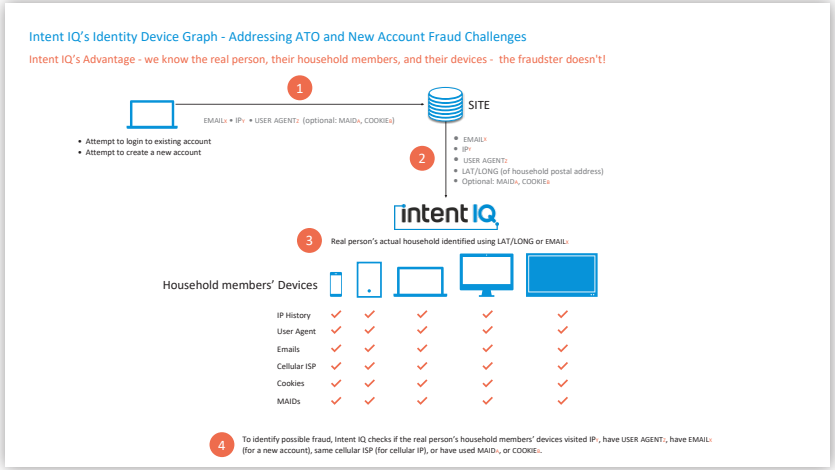
**Once integrated, the following client support options are offered:**

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

# Intent IQ



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




## Key developments over the past 12 months.

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

- **Intent IQ** introduced Mobile Identity Hub ('MIH'), its ID solution for MAID-less environments, such as the one created by IDFA deprecation or AAID future elimination, by stepping-in and providing a privacy friendly universal ID that facilitates cross-app targeting and attribution. **Intent IQ's** solution is in line with the online advertising industry standards and in compliance with the law (incl. CCPA). Originating from the people that invented and evangelized AdChoices, privacy is in Intent IQ's DNA. MIH leverages **Intent IQ's** experience in providing accurate and scalable solutions to cookie-less environments.
- A patent-pending cross-app attribution solution, ATTLICA™. When a client's IDFA-less data is assigned to a device by **Intent IQ**, the data is immediately turned into aggregated data, to avoid device-specific cross-app attribution. This aligns with Apple's App Store privacy and data use practices. However, unlike SKAdNetwork, Intent IQ is able to provide the same granular attribution post-iOS 14, in scale and with the same accuracy as pre-iOS 14, along with a months-long attribution time window.

**12-month roadmap**

In the coming year, **Intent IQ's** ability to identify a device using only an IP address and the user agent originating from the device will become more important than ever. Validating device user-claimed credentials will be crucial given Apple's expected deprecation of IDFA in early spring 2021 and Google's expected elimination of third-party cookies in early 2022, combined with browsers expanding blockage of device fingerprinting.

To further facilitate the above, in conjunction with Google elimination of third-party cookies, Intent IQ is expected to release a browser identification solution.

# Neustar

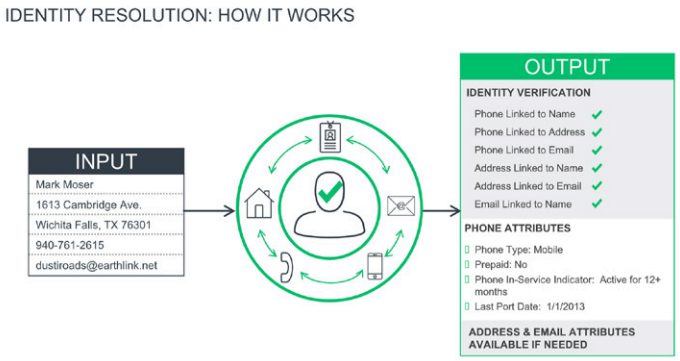


**Neustar** helps companies efficiently connect with customers while mitigating their fraud and compliance risk. **Neustar** fraud and authentication solutions provide the "unspoofable" consumer insights needed to know with certainty who is at the end of every interaction, creating trusted and frictionless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

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

## Solutions and Functionality

To **Neustar**, "identity resolution" means using a host of authoritative identity signals to quickly identify, authenticate, and fast-track legitimate customers and interactions while mitigating against the negative impact of fraud. The more accurately consumers can be



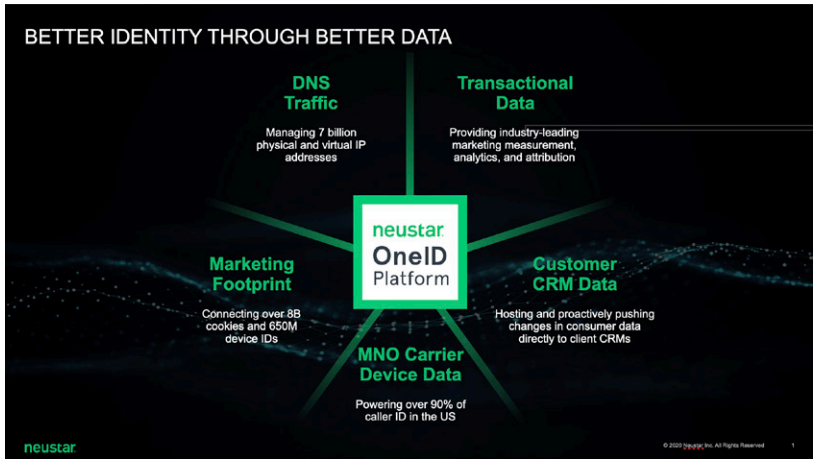

neustar®

### 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

identified, the harder it is for malicious users to spoof identities and take over accounts. It ultimately makes better decision-making possible, along with a more frictionless consumer experience. Neustar works with and provides identity intelligence to the top 10 leading banks, the top 10 leading card issuers in the U.S., and some of the biggest brands across every industry and vertical.

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




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

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

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

There are four primary product offerings:

**Digital Fraud**

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

With these elements, they corroborate the digital information against offline consumer data and provide organizations' decisioning engines with additional, differentiated data that can help indicate the trustworthiness of the digital identity. Predictive scores based on machine-learning models provide easy-to-understand signals for fraud mitigation.

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:

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

**Account Takeover Fraud**

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

- **SIM Swap** helps to identify cases where a mobile phone number has recently become associated with a new SIM card. SIM-swapped phones are frequently used in account takeover attacks.
- **Call forwarding** allows users to confirm whether the number is being forwarded, and in many cases, to whom it's being forwarded. Because of the access to offline data (associated addresses), this service can confirm both high- and low- risk forwarding.

# Neustar



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

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

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

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

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

# Neustar



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

Target user groups include large inbound call centers, as well as financial, insurance, government, retail/ecommerce, healthcare, 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 and a customer success contact. Direct API integration can typically be achieved within a week, depending on the needs and setup of 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** is a leading provider of online identity information. Their products and services are used by top ecommerce businesses, financial and insurance institutions, and governments around the world to provide frictionless customer experiences and reduce investigation times.

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

## At a Glance:

3rd Party API Capabilities


Professional Guidance/Services


Pre-Authorization Functionality

## Solutions and Functionality

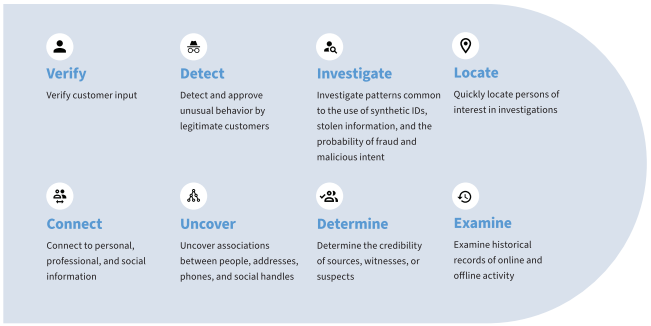
Primary solution offerings fit into two distinct categories:

- **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 specific locations, emails, people, and businesses. Conversely, it can help determine if the buyer is likely to be using false or synthetic identity information. This reduces manual review times across the entire fraud team.Key performance indicators (KPIs) of focus through the manual review solution include: case time/operational cost, case resolution rate, verification accuracy, and reduced customer insults.
- **Pipl API for Automated Identity Verification: Pipl 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, and reduced customer insults.

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 this is provided at no cost to the customer after speaking to their dedicated account manager.
- **API:** To ensure success, a dedicated customer success engineer performs a data evaluation plan with the customer at no charge. "What if" analysis is available by utilizing a test file (xls, csv, etc.). After integrating **Pipl API** into their test environment, customers have access to robust online identity information as well as source and timestamp metadata that provides a historical record of the identity.




## Reporting

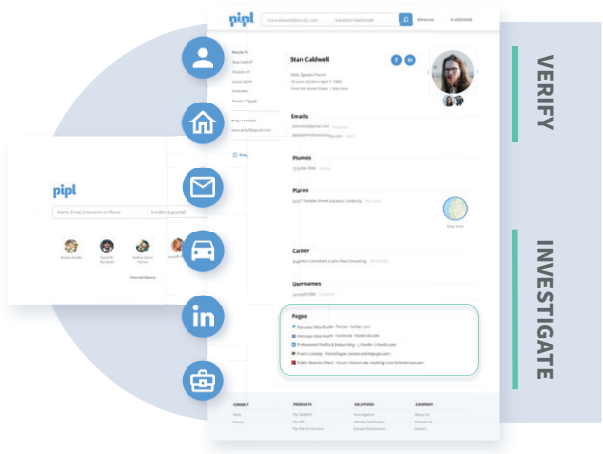
**Pipl** customers are assigned dedicated account management resources to help customize the reporting of SEARCH and API products based on the unique requirements of the customer. This may include metrics such as:

(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:** An annual license fee applies per user, with unlimited searches
- **API:** Transaction-based
- Custom pricing and packaging options are also available

## Integration Options

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

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

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

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

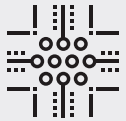
SOCURE

## At a Glance:

Machine Learning

Device Fingerprint Capabilities

Pre-Authorization Functionality



Non-Production Real Time Rules Testing

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

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

## Solutions & Functionality

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

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

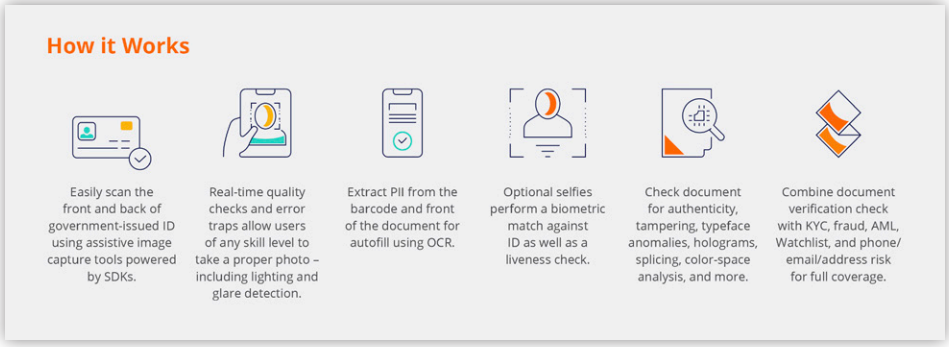
Their identity element-specific machine-learning models are trained with 50+ element-specific variables to predict the likelihood of fraud and risk by leveraging validity, correlation, age, risk, activity, and more. **Socure's** service has greater than 96% coverage for emails, phones, and addresses.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

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

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

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

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




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

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

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

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

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

## Services and Integration

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

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

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

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

## Vertical Markets

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

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

# TeleSign



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

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

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

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

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

## At a Glance:

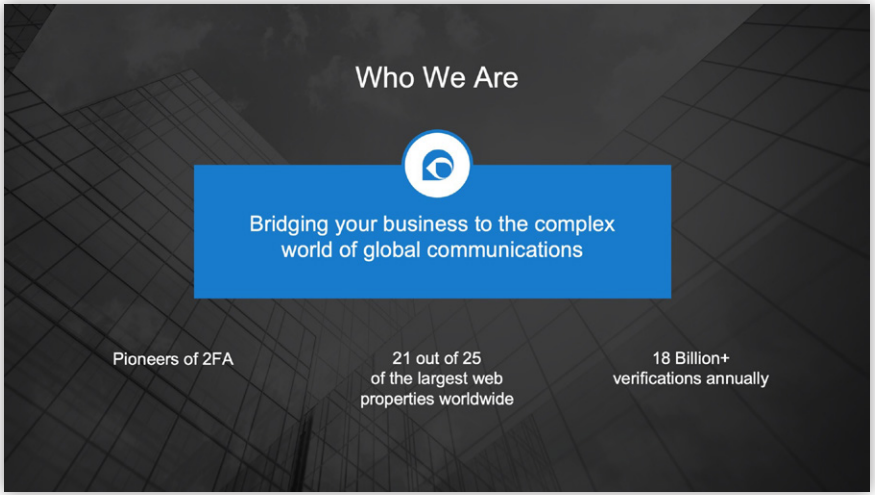
ATO Detection Capabilities

Account/Client Management

Pre-Authorization Functionality

# TeleSign



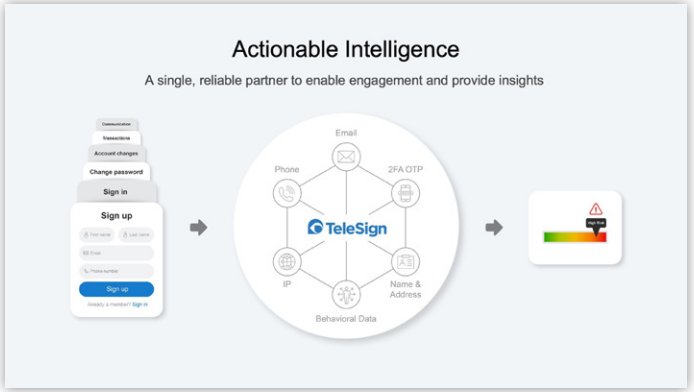



## Primary Products and Services:

**Phone Score**

This service delivers reputation scoring based on phone number intelligence, traffic patterns, machine learning, and a global data consortium. Associated insights include:

- **Phone Number Data & Analytics:** Phone number data attributes (including phone type, telecom carrier, account and device ID and IP address) are evaluated to identify potential fraud risk.
- **Global Fraud Data Consortium:** This score leverages two global databases to help detect and identify known fraud faster.
- **Traffic Pattern Recognition & Usage Velocity:** This identifies anomalous traffic behavior patterns and usage velocity that may raise red flags.
- **Machine Learning:** This trains algorithms to uncover hidden insights in data to predict fraudulent or high risk phone numbers. Customized machine-learning models that use customer-provided data further increase the effectiveness and accuracy of Phone Score's fraud detection capabilities.
- **Evaluation Of Customer-Provided Data Inputs:** This machine-learning model can also evaluate unique customer-provided data inputs such as user IP address, email address, account ID, and device ID with each API request to further increase the effectiveness of risk assessments, specific to the customer's environment.
- **Actionable Risk Assessment Recommendation:** A data-driven risk assessment score is designed to help determine the appropriate action of whether to allow, block, or flag a registration or transaction. The score can be used as a standalone solution, integrated with other solutions, or combined with SMS to challenge users when flagged.



# TeleSign



**Phone ID API**

Phone ID API offers detailed and actionable global phone number and subscriber data intelligence to strengthen authentications, evaluate fraud risks, and enhance the user experience. Phone number data intelligence can help strengthen the user verification process, reduce fake accounts, inform risk models, improve conversions, and determine the optimal channel for message delivery. The PhoneID API cleans and reformats a submitted phone number and returns phone device-type, telecom carrier name, and phone registration information. Additional data attributes are available for configuration via add-ons to best fit your specific use case. Associated insights include the following:

- **Contact:** End-user phone number intelligence and contact information (first and last name, street address, city, state), based on carrier subscriber contact data. Use to strengthen existing fraud risk models and improve registration UX with pre-filled form fields. (U.S. only.)
- **Number Deactivation:** Provide end-user phone number and receive data intelligence on when a phone number has been truly deactivated, based on carriers' phone number data and TeleSign's proprietary analysis. Delivers a date and time stamp in the event a trust anchor has been broken.
- **Contact Match:** Provides end-user phone number data, first/last name and address, and a score of 0-100 as matched against carrier subscriber contact data. Validates an end-user's physical address at onboarding, during a high-value transaction, when verifying a shipping address, and to strengthen existing fraud risk models.
- **SIM Swap:** Find out whether the SIM for a phone number has been swapped, and if so, at what point. TeleSign evaluates how likely it is that the SIM swap was for a fraudulent reason using a scale from 1 to 4.
- **Subscriber Status:** Provides end-user phone number and receives current carrier subscriber status (account activation date; prepaid or postpaid; active / not active, suspended, account type; primary account holder; length of account tenure; and date of last status change) to understand the strength, value, or risk of a user.
- **Porting History:** Provides end-user phone number and number porting history data for the last 90-days to prevent account takeovers. This reduces the creation of fake and fraudulent accounts and improves operations.
- Porting Status: Provides end-user phone number and information on whether the number has been ported or not and what carrier currently has the number.

**TeleSign** products support organizations through the following use cases.

# TeleSign



### Streamlining account creation

Digital identity can provide a seamless onboarding and secure buying experience for end-customers. At the same time, timely and relevant SMS and voice communications get viewed instantly, keeping your business top-of-mind and building stronger relationships and loyalty with buyers. From instant order updates to discount offers and two-factor authentication messages, **TeleSign's** platform is changing the way ecommerce businesses engage customers and prevent fraud.

New web and mobile app users are converted quickly by collecting a phone number, verifying that it belongs to the account registrant, and using phone number intelligence to assign a fraud risk score. Bad users are identified and challenged or blocked.

### Reduction of fake accounts

Companies can confirm the identity of end-users by attaching a verified mobile number at account registration. Phone number intelligence can be provided to evaluate the potential risk of the end-user.

- Collect a phone number at account registration and assess fraud risk.
- Challenge or block suspicious accounts through SMS or voice-based one-time passcodes.

### Account Takeover (ATO) Prevention

From login to logout, accounts can be continuously secured from compromise with minimal user disruption. Even if a hacker is in possession of a user's correct account credentials, two-factor authentication (2FA) can prevent unauthorized account access and activity.

Challenge suspicious account activity:

- Login attempts from a new location, device, or browser
- Password resets
- High-value transactions
- Changes to account details or personal information

### Know Your Customer (KYC)

Gain a deeper understanding of your customers from actionable global phone number and subscriber data intelligence. It's more important than ever for online businesses to truly understand their customers on a deeper level to meet their evolving expectations and achieve compliance with Anti-Money Laundering (AML) regulations. TeleSign helps organizations "know their customer" by accessing real-time behavioral, phone, and user analytics.

### Minimize Fraudulent Transactions

Utilize data intelligence and two-factor authentication to verify transactions and distinguish good users from bad. Phone verification using number intelligence to develop a fraud risk score at account

registration helps block fake accounts by identifying good users from potentially harmful ones. With 2FA enabled, notifications can be triggered to approve, challenge, or deny transaction activity.

Confirm user identities and activity through:

- Phone verification
- Fraud risk scoring
- PIN challenges
- Push notifications

**Enable Secure Account Recovery**

Streamline secure password resets and reduce help desk calls by sending a one-time passcode to the verified phone number on record via SMS or a voice-based call.

By automatically sending a secure one-time passcode (OTP) to the verified phone number on record, the account recovery and password reset process can help reduce support costs and protect end-user accounts from compromise.

## Pricing:

Several variables dictate pricing, but the typical pricing format is transaction-based with a monthly minimum.

## Developer Guides:

Standard: Products for small teams, pre-paid through self-service portal.

Enterprise: Products for larger organizations, invoiced monthly.

# Flashpoint



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

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

FLASHPOINT

## At a Glance:

ATO Detection Capabilities

Pre-Authorization Functionality

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

# GB Group



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

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

GBG

## At a Glance:


3rd Party API Capabilities

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

# 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.

# Oneytrust



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

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

oneytrust

## At a Glance:


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

# Onfido



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

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

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

onfido

## At a Glance:

Machine Learning

ATO Detection Capabilities

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

# Chargeback Management & Platforms

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

# Accertify Chargebacks



**Accertify** 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 allow clients to address risk pain points across the entire customer journey. From account creation to authentication, activity monitoring, payment, and disputes, risk is mitigated 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.

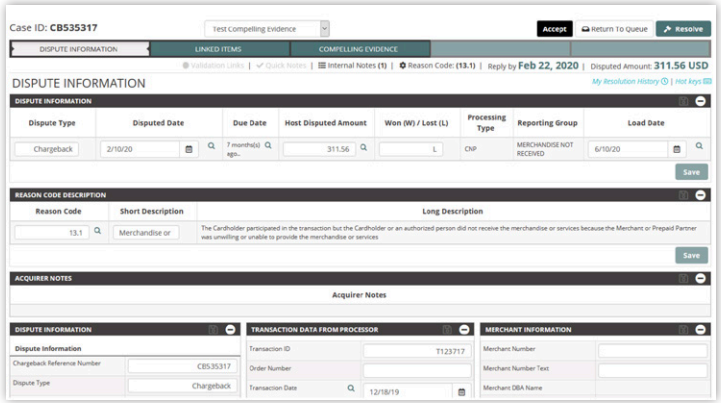



Figure 1: User Interface

AN AMERICAN EXPRESS COMPANY

## At a Glance:

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

# Accertify, Inc.



**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 they 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, without human intervention, into the platform. Chargeback responses can also 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.

  **Accertify's** automated document capture process 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, it 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 if 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 can also show an agent's average work duration for a specified period. Won/loss ratios can also be aggregated and grouped out by a reason code group, brand, and processor for trend analysis.

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

- **Solution Integration: Accertify's** Chargeback Management solution is directly integrated with the Fraud Platform; information is automatically populated into the Chargeback Management solution and vice versa. Fraud and chargebacks form a symbiotic relationship. Because each can seamlessly leverage and benefit from each other, they stay synchronized and realize their maximum potential. **Accertify** also partners with Ethoca and American Express, receiving chargeback alerts in near real-time. This allows clients to react to change faster, including potentially stopping shipments and issuing refunds. It helps improve prevention rules, strategies, and model performance—and provides a better customer experience.

# Chargeback



**Chargeback** is a Salt Lake City-based company established in 2011. They offer fully automated responses, self-managed responses, and managed services to cover any business need. Their focus is using automation to help simplify the process regardless of which path is chosen.

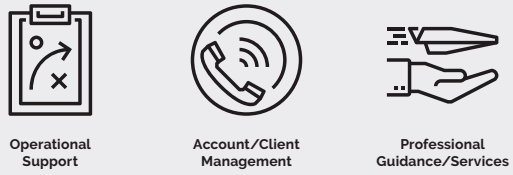
The drive behind this focus: the increased need to provide real-time dispute responses to issuers and networks. **Chargeback** believes that the Visa Claims Resolution (VCR) and MasterCom Dispute Resolution initiatives will drive this need even further.

## 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. It can be time-consuming and cumbersome to decide whether or not to respond to a dispute, determining what evidence to provide, and then compiling that evidence. 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 the data their merchant clients need without requiring clients to 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.

Another feature of the app is that it automatically updates to include any changes in rules or regulations that the issuer may require. It can also automatically adjust information based on reason codes and modifiers so anyone can work through a dispute, not just an expert.

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 the dispute page, 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.

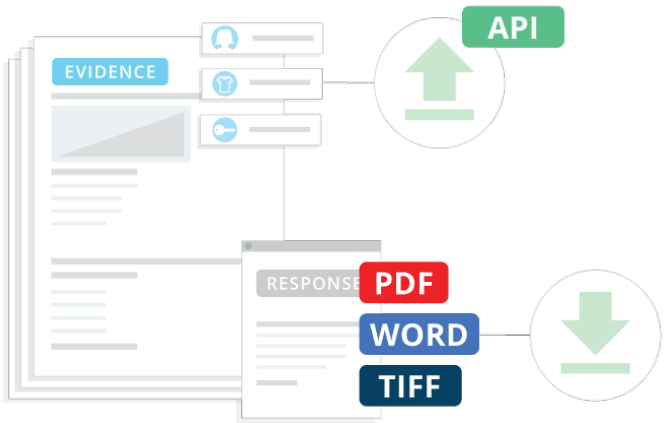
The **DocGen** automation in the **Chargeback** app provides a response generator, which can collect order, customer, transaction, and dispute data and add it to auto-populated responses.
The responses address specific requirements outlined in Visa, MasterCard, American Express, and Discover rules and 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. In addition, the app can provide supporting information from fraud filter integrations to maximize evidence. And in the case of actual fraud, feedback loops can provide information back to the fraud filters about why the dispute was lost.

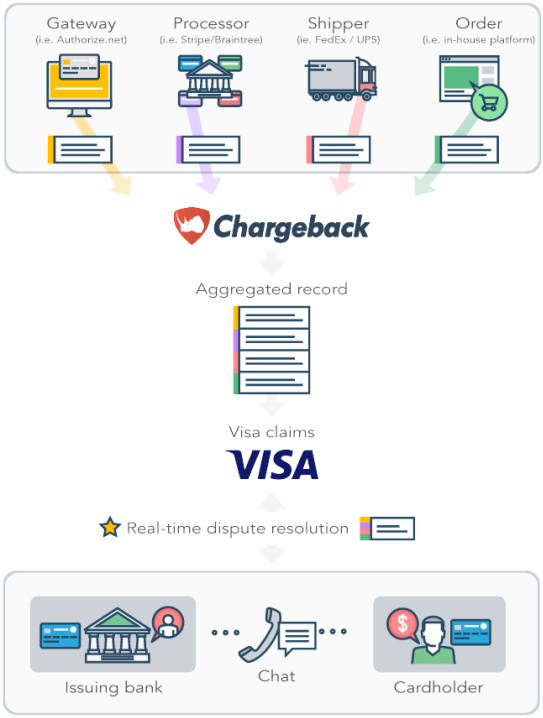
Once complete, the support documents are created and submitted automatically using another automation tool inside the app called **DocSend**. It auto-sends completed responses in PDF or Word formats by email, fax, or upload, depending on requirements.




Through the application, merchants benefit from another automation tool: **Real-time Resolution**. This functionality allows merchants to provide customer, order, and product detail to the card brand dispute management platform—Visa Resolve Online (VROL) or Ethoca Eliminator. This supplemental information is combined with the related card brand transaction data and made available to the dispute analyst at the cardholder's issuing bank. With this enhanced level of detail, the dispute analyst is equipped to make 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 detail, order detail, and product detail is not made available until well into the dispute process and can be accompanied by a message that a credit has been issued. This can also allow organizations to deflect many friendly fraud disputes as well as chargeback fraud disputes that will be difficult to win.

# Chargeback






Through integrations with Ethoca and Verifi, 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. The integration allows users to be notified earlier in the process than they would otherwise. Users know as soon as the card companies know a dispute has been filed. These notifications enable the merchant to initiate time-sensitive actions such as stopping fulfillment, deactivating gift cards, 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. They offer dashboard views of dispute overviews, RTR overviews, and alert overviews. They also offer downloadable reports for all three with more in-depth data. This is all included with the product.

The current focus is on giving clients the data they require to make sure their dispute management program is efficient and working for their business needs.

## 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, WorldPay, Stripe, Braintree, Authorize.net, and NMI (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:** Much of this functionality is live as of publication of this report; soon, the remainder will move beyond beta testing. The functionality includes 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 representment documents to processors.
- **DisputeBot** offers fully automated responses to chargebacks based on set circumstances. For example, disputes under a specific amount can be automatically handled to be refunded. Automatic dispute responses can be filed for disputes that fall within specific requirements that a company can set. The rules can be set up to allow merchants to focus on other aspects and only deal with the most complicated disputes.
- **Data analytics:** Merchants gain report visualization, including charts and graphs. Additional reporting options include 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.

# ChargebackOps



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

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

**Primary differentiators include:**

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

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

## At a Glance:

Operational Support

Account/Client Management

Professional Guidance/Services

# ChargebackOps




**Keep authentic shoppers and build long-term customers.**

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

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

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

**ChargebackOps** offers two primary services:

- **Chargeback Management Service: ChargebackOps** offers a uniquely designed dispute resolution service for Fortune-500 ecommerce companies who prioritize the lifetime value of their customer and their brand. Using a hands-on and collaborative approach, their analysts investigate and respond to each chargeback case in order to optimize the client's desired handling for all types of fraud.
  For this reason, they do not use the one-size-fits-all approach found commonly with automated systems. They rely on human intelligence to provide customized handling for each client. The chargeback analysts work as an extension of their client's internal fraud team. The intelligence is gathered and shared with clients to identify problematic fraud trends and build new fraud rules to avoid excessive chargebacks. **ChargebackOps** handles 100% of the chargeback response process and provides clients the analytics to track and report progress.

# ChargebackOps



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

  They review and cross-reference over 30 data points in order to provide a conversion rate better than 90%. The expert teams help clients exceed their fraud goals at an optimized price. With order screening and chargeback management service, they operate on both sides of the ecommerce transaction. When using these services together, **ChargebackOps** offers clients with a unique fraud viewpoint, measuring and scoring both order screening quality and opportunities to further develop fraud rules. With screening analysts dedicated to each client, they can score and treat each order in a customized fashion, providing customer service experiences similar to that of a client's own employees. Rules development and management support is provided; however, **ChargebackOps** aims to empower clients to manage their own rule management process. Significant data, close collaboration, conversations, filters, and rule recommendations are provided on a regular basis. Additional ad-hoc feedback is provided by agents who review chargebacks, identifying and relaying fraud trends back to merchant clients. The feedback loop is a true differentiator. Three types of reporting are currently available, all included in the price of the service.

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

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

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

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

## Proof-of-concept process:

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

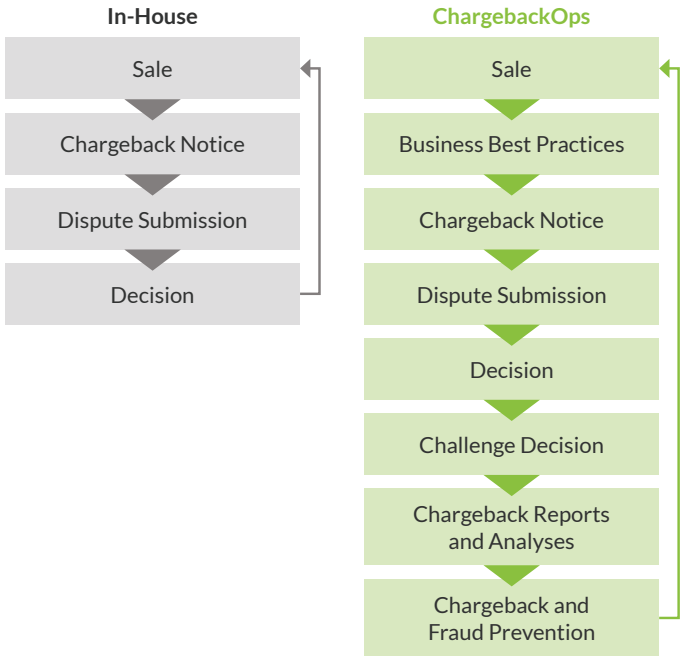
## Pricing Models

### Chargeback Management

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

### Order Screening & Review

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



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

**Integration**

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

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

Their 12-month roadmap includes several new significant partnerships in 2021.

# 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

## 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.

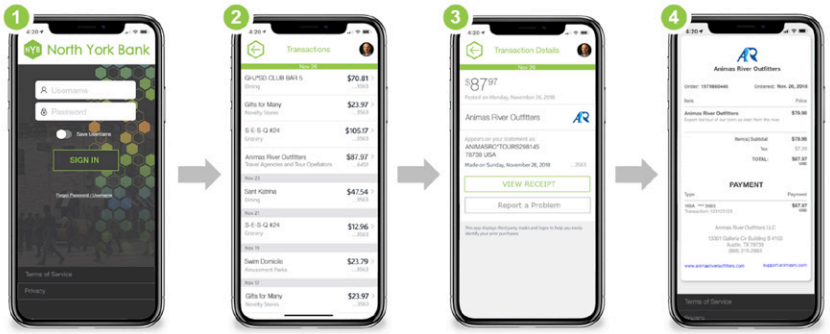
**Ethoca's** onboarding integration team works with customers to develop integrations. Merchants can code to the Application API and go live, which is the same for **Accertify** and **Kount**. The issuers integrate into a separate API, or may choose to provide intraday, file-based delivery to get data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

Operational Support

Account/Client Management

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

# Verifi



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

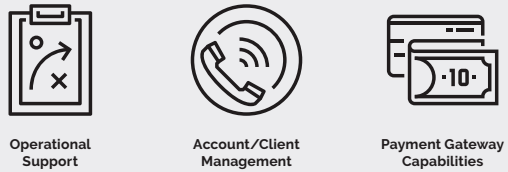
Verifi states they offer the following solutions:

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

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

VERIFI

## At a Glance:




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

paladinfraud

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

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