paladin vendor report | **fraud prevention**

Thank you for downloading the Paladin Vendor Report.

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

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

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

Sincerely,

The MRC

Table of Contents

The 2024 Paladin Vendor Report

In the cat-and-mouse game of fraud prevention, this report puts you a step ahead. Information is the key to prevention. It's what we've learned in our decades of work as fraud prevention consultants, during which we've witnessed every scheme fraudsters could cook up—and we've studied every technology aimed at combating their efforts. Immersed in the day-to-day world helping merchants manage their fraud challenges, their personnel, and their platforms, Paladin is in a unique position to write this report. It's our job to stay up to date on technological advancements in the industry as we help organizations mitigate transactional and identity risk.

As the number of providers and services grow and technology evolves, merchants' options become increasingly complex and varied. Our mission is 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. It's why we published the first-ever Paladin Vendor Report (PVR) years ago and have issued an updated annual report ever since—giving the industry an unprecedented exploration of how merchants could mitigate the risks that come with accepting payments in an omni-channel, card-not-present world.

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

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

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

Introduction

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.

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.

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

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

Using data gleaned from the behavior of a population of normal users, **BehavioSec** can help you quickly pinpoint fraud, whether bot or human.

Checkout Fraud

Using metadata from normal behavior and previous customer interactions, **BehavioSec** can detect fraud without adding friction. It allows merchants to focus on improving customer experience and conversion rates.

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.

Featurespace

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

Solutions & Functionality

Featurespace's technology attempts to mimic a human-like ability to profile people over time through the ARIC platform, which uses their proprietary Adaptive Behavioral

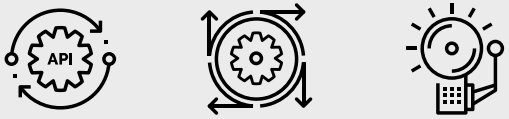
Analytics and Automated Deep Behavioral Networks to model and predict real-time individual behavior. This functionality allows computers to understand when an individual customer's behavior is out of character; the platform then automatically evaluates the risk. The technology can be deployed on-premise or via secure cloud, and it is scoring transactions from over 180 countries. In 2018, the ARIC platform risk-scored an estimated 15 billion transactions worldwide.

ARIC's tiered, multi-tenancy solution 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.

FEATURE SPACE

OUTSMART RISK

At a Glance:



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

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

Neuro-ID

Neuro-ID segments fraudulent digital applicants from genuine future customers through advancements in behavioral science. Via a JavaScript integration, Neuro-ID collects behavioral signals from web and mobile applications, then processes these signals, in-session, to inform real-time decisioning. Neuro-ID customers receive scores ("Neuro Confidence Scores")

and attributes ("Neuro Attributes"), thereby gaining behavior-based insight into every digital applicant. Neuro-ID's scores and attributes offerings are accompanied by a dashboard, giving companies insight into previously unknown end-user behaviors. These behaviors indicate intent as well as emotion and experience during the course of a digital customer journey.

Neuro-ID helps support improvements of the following KPIs:

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

Neuro-ID operates in the digital onboarding environment, account creation, account management, and account access. They are expanding rapidly into ecommerce and have a successful history in lending, payments, buy-now-pay-later, and insurance. The technology helps organizations "optimize friction," which means that not only are bad transactions caught—but also, more good transactions are identified and accepted, supporting improved conversion and higher revenue totals. Consequently, Neuro-ID moves risk management teams from cost centers to revenue generators and, in many cases, opens additional market opportunities that are historically seen as high-risk.

NEURO-ID®
HUMAN ANALYTICS™ FOR THE DIGITAL WORLD

At a Glance:

3rd Party API Capabilities

Pre-Authorization Functionality

User Behavior Capabilities

Neuro-ID 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.

NuData Security, a Mastercard company

NuData Security, a Mastercard company, helps businesses validate good users without disruption and stop bad actors before they can cause damage. With over 20 billion risk assessments processed and 4.5 billion devices seen yearly, **NuData** harnesses the power of behavioral signals and device intelligence to verify users, stop account takeover, prevent new account fraud, and reduce good user friction in real time.

Solutions & Functionality:

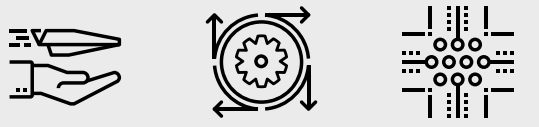
NuDetect is a multi-layered solution that combines behavioral biometrics, analytics, device intelligence, and cross-client consortium data to recognize good user behavior and pinpoint anomalies.

By passively analyzing digital behavior at a user level and population level, **NuData** provides clients with risk scores in real time, allowing them to avoid unnecessary challenges for good users and block high-risk traffic before damage occurs.

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

NuData Security
mastercard

At a Glance:



NuData 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.

Shape Security

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

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

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

Their primary goal for merchants is to protect against:

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

At a Glance:

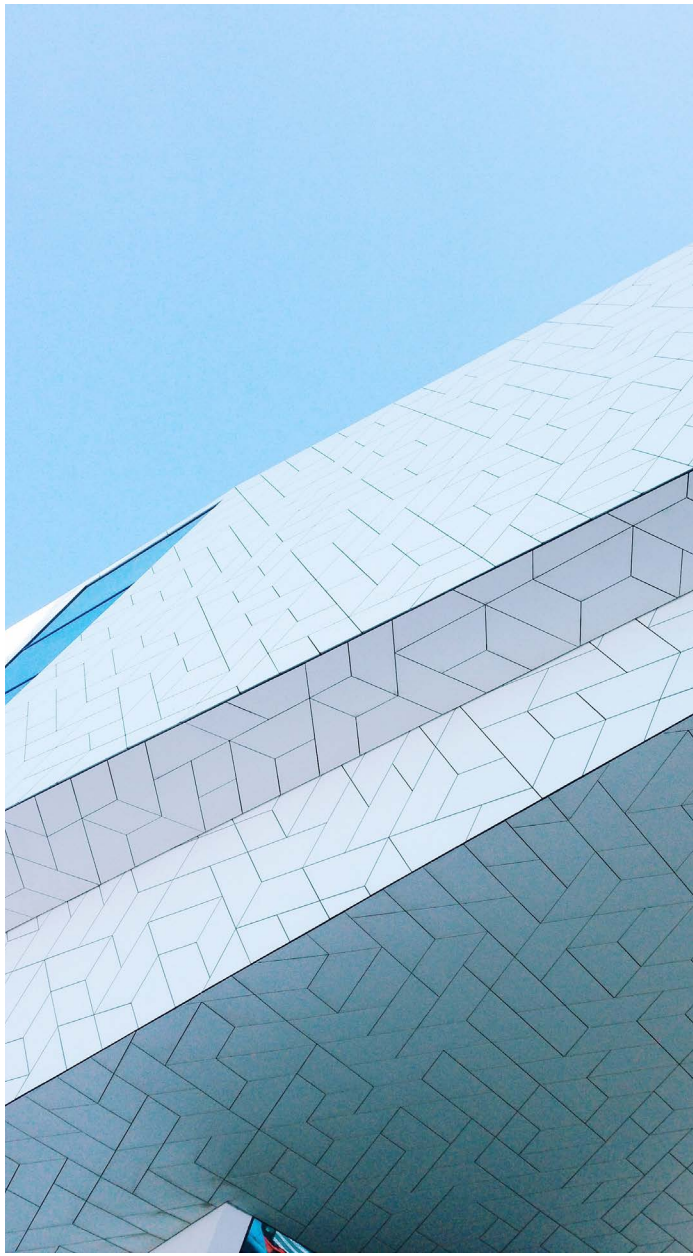
User Behavior Capabilities

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

3DS & Consumer Authentication

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

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



Accertify 3D Secure

Accertify provides fraud prevention, chargeback management, Account Protection, refund and returns, Strong Customer Authentication (PSD2), 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 make it possible for clients to address risk pain-points across the entire customer journey—from account creation to authentication, activity monitoring, payment, and disputes.

Accertify's 3D Secure (3DS) Solution

Accertify's 3DS solution is available as a stand-alone authentication product or as part of their end-to-end authentication management solution. The 3DS solution supports both EMV 3DS 2.1 (3DS2) and 3DS2.2. 3DS1.0 has been in the process of being decommissioned around the world, but **Accertify** supports this version in regions where specific waivers were granted. **Accertify** is further supporting the additional authentication approaches outlined in 3DS2.3 with Accertify's FIDO (Fast Identity Online) authentication technology.

Accertify

At a Glance:

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

Accertify 3D Secure

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

The Frictionless Flow and the Challenge Flow

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

Fraud Liability Shift

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

Additional Protocols

The frictionless flow, challenge flow, and declined authentication flows as described above have been in place for a few years. But the infrastructure that supports these flows has evolved considerably over time. The initial version of 3DS, 3DS1, was launched in 1999 by VISA. The 1.0 protocol proved successful in reducing ecommerce fraud, so similar protocols were created by other 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 was a significant evolution from 3DS1— the primary enhancements include:

- **Data sharing:** 3DS2 shares ten times as much data as 3DS1. This includes device, session, and IP data. This data enables the issuer to make better decisions when assessing the authentication request.
- **Mobile app optimization:** 3DS2 is designed to work with both a browser and app/device-based shopping experience.

For example, 3DS2 can be implemented seamlessly into the merchant app, providing a much more customer-friendly experience.

- **Non-payment based authentication:** 3DS1.0 was limited to payment flows, but 3DS2 supports non-payment flows. For example, 3DS2 can be used to authenticate the provisioning of a card into an e-wallet.
- **Tokenization:** 3DS2 supports tokenized transactions, which helps to reduce the risk of the card number being compromised.
- **Support for a variety of authentication methods:** This includes one-time passcodes, biometrics, and out-of-band authentication.

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

Merchant Fraud Strategy

Accertify believes that 3DS2/2.2/2.3 should be an essential part of a merchant's fraud strategy. 3DS2 not only brings financial benefits through fraud reduction and fraud liability shift, but it can also help to protect merchants' brands by ensuring customers feel secure when making purchases via app or website.

Strong Customer Authentication (SCA)

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

1. Inherence (such as biometric)
2. Possession (such as device)
3. Knowledge (such as PIN/Password)

For the time being, the scope of SCA is limited to cards issued within the European Economic Area (EEA), and there are exemptions available. At a minimum, all ecommerce merchants based in the EEA should implement 3DS as part of their compliance strategy in meeting the enforced EEA regulation requirements. A merchant's failure to comply with the EEA regulation may cause a significant number of sales to be declined by the respective card issuers.

SCA, as per Payment Services Directive 2, is currently only enforced in Europe. However, similar regulations have been observed in other jurisdictions around the world and continue to be. **Accertify** can support merchants present in any region where authentication mandates have been deployed; **Accertify** believes that merchants should not only implement 3DS, but they should also implement

an SCA optimisation solution. **Accertify's** solution enables the merchant to maximise all the available exemptions and scope criteria to ensure as many sales as possible are processed without the potential for friction associated with 3DS. Identifying payments that are out-of-scope or exempt, can help the merchant provide the optimal customer experience, reduce overheads, and increase conversion rates.

While 3DS1 supports SCA compliance, its imminent decommission means merchants should integrate 3DS2 and its newly available versions as a priority. 3DS2 is a substantial improvement from 3DS1 and provides the merchant with the ability to share more information about the payment and SCA-related information such as exemptions, mandated challenges, etc. Not only does 3DS2 carry more new data points, but it also enables the latest authentication options, such as Secure Payment Confirmation and Delegated Authentication. **Accertify** believes these new authentication technologies are pivotal to reducing cart abandonment.

The authentication technologies are powered by FIDO (Fast Identity Online) to provide the user with passwordless authentication experiences. FIDO lets the user authenticate themselves using their device and biometric, using standard public key cryptography. **Accertify's** FIDO authentication technology can be used in these solutions, reducing payment friction and reliance on SMS/OTPs.

Cybersource's 3-D Secure Solution

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

Decision Manager plus Payer Authentication

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

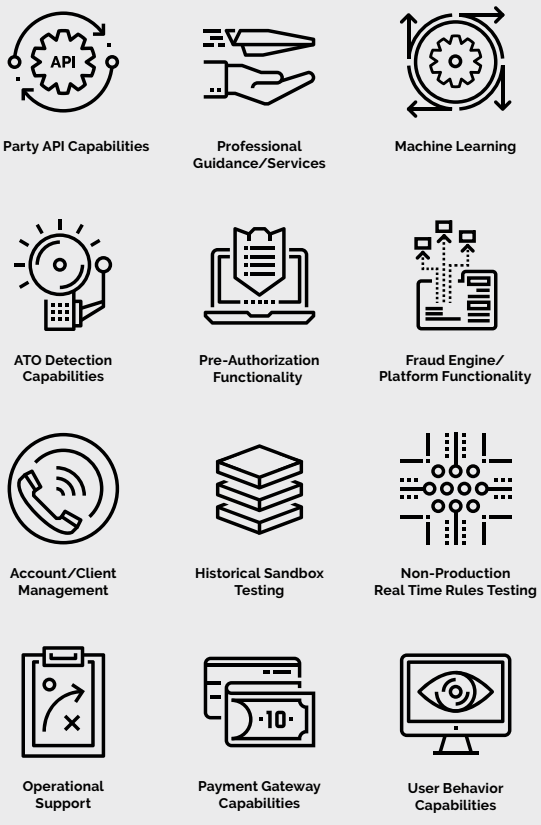
Payer Authentication

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

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

cybersource
A Visa Solution

At a Glance:



CardinalCommerce

CardinalCommerce is a payment authentication provider offering a suite of payment decisioning solutions. **Cardinal's** goal is to make authentication a trusted standard for everyone within the digital commerce ecosystem by offering solutions that provide the data that organizations need when they need it. Since 1999, **Cardinal** has been offering payment authentication and is an EMVCo member, playing an active role on their business and technical committees. **Cardinal** works with merchants and issuers to deliver a trusted, often frictionless experience for everyone in the digital commerce ecosystem. They develop solutions to simplify and accelerate authentication for their customers and their customers' customers.

Through the **Cardinal** Exchange, they can offer merchants and issuers visibility to both sides of the transaction and access to more actionable data, which can positively impact the decision-making process, Through shared data, merchants may receive benefits like reduced false declines and fraud, increased authorizations, improved customer experience, quicker response times, and more control over step-ups, which can result in more authorizations.

At a Glance:

3rd Party API Capabilities

Pre-Authorization Functionality

Account/Client Management

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

Outseer 3-D Secure™

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

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

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

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

OUTSEER
An RSA Company

At a Glance:

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

Device Identification, Recognition & Reputation

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

ThreatMetrix

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

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

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

ThreatMetrix

At a Glance:

Device Fingerprint Capabilities

Fraud Engine/ Platform Functionality

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

Fraud Platforms & Decision Engines

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

Accertify, Inc.

Accertify provides fraud prevention, chargeback management, Account Protection, refund and returns, Strong Customer Authentication (PSD2), 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 make it possible for clients to address risk pain-points across the entire customer journey—from account creation to authentication, activity monitoring, payment, and disputes.

Solutions and Functionality

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

Accertify

At a Glance:

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

Accertify, Inc.

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

Scoring: At its core, the Interceptas® Platform is a data management tool. By offering a rich set of integrated machine learning models, pre-built rules, and condition checks, clients can implement a near-infinite range of policy checks to live alongside their fraud screening strategy. The user-friendly interface is designed to allow non-IT resources to author rules and make comparisons to adjust risk assessment.

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 most of the 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.

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

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

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

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

Core features include:

- **Malware and crimeware detection:** Analyzes connected devices to detect known malicious applications and criminal tools, such as location spoofing and IP address proxy apps. Malware files are dynamically updated without client interaction.

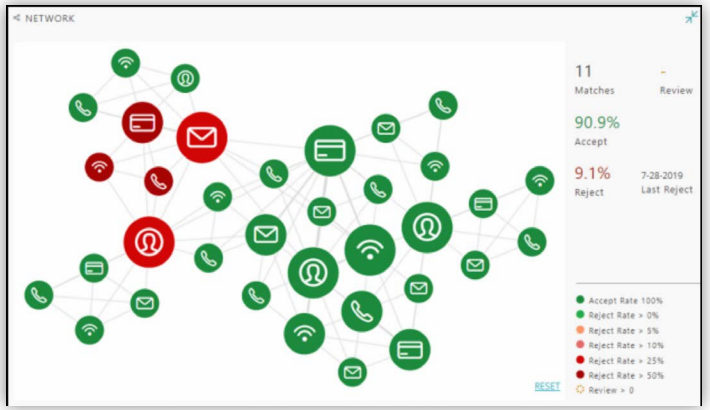
- **Rooted/Jailbroken detection:** Protects against increasing—and increasingly complex —rooting methods used by fraudsters, such as cloaked Root, through Advanced Root and Jailbreak Detection.
- **Trusted Path:** Security architecture prevents interceptions by providing a complete secure path to transport sensitive information, encrypted end-to-end, signed, and digitally protected against replay attacks. Trusted Path securely communicates sensitive messages.
- **Secure messaging:** Secure means of delivering contextual Two-Factor Authentication (2FA) messages to a registered device through the SDK and secure Trusted Path that cannot be read by any other device, intercepted, or replayed. This can be a stand-alone offering.

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

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

User Behavior Analytics (UBA): Accertify offers clients the ability to track the behavior of their customers' web traffic using their UBA solution. By analyzing behavioral signals from users as they interact with client's websites, UBA can help distinguish good users from fraudsters and detect suspicious activity from humans or bots. The solution provides 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 the client the ability to search for historic linkages that can clarify whether an event is out of pattern, or is evidence of a loyal, repeat customer. The capability is flexible in what values can be displayed and searched and offers power users the ability to perform batch exports, execute data pivots, and bulk resolution capabilities.



Accertify, Inc.

Rules/Conditions Testing: Clients can test and simulate a condition or conditions using the **Accertify** rule testing "sandbox." The functionality in the sandbox provides the ability to look historically and get an analysis of a proposed rule change. For testing conditions on current and future transactions, a client can run tests in the production environment and set a passive score where it wouldn't affect the outcome.

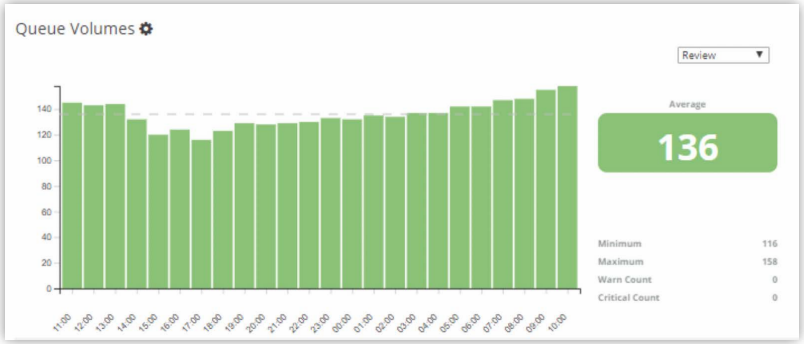
Profile Builder: Identifies real-time patterns and trends through the dynamic summarization and aggregation of data. Gives insight real-time at the transactional level to discern fraud rates, track new product launch limits, monitor account usage, analyze customer buying patterns, and uncover organized fraud rings. 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.

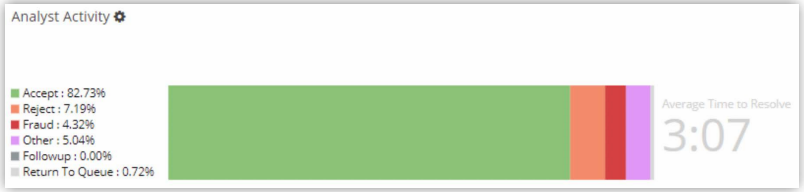
Chargeback Management: Please see full write-up in the **Accertify** Chargeback section of the Paladin Vendor Report.

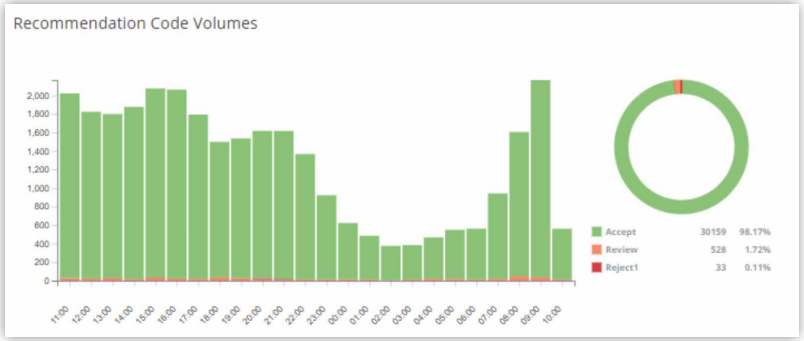
Payment Gateway: This complementary product is for clients seeking a singular platform for payments and fraud. The **Accertify** Payment Gateway is processor-agnostic, giving merchants the flexibility to select different processors for different payment types, and it provides easy connectivity to multiple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

Reporting: Accertify offers three types of reports.

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

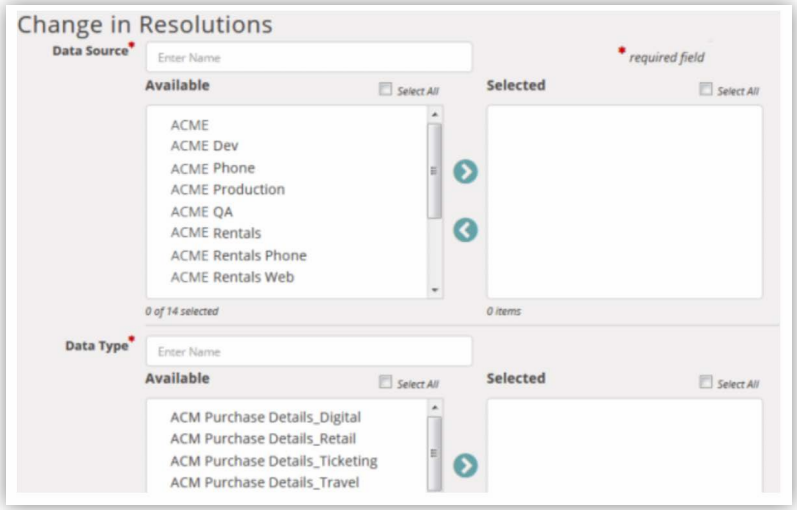




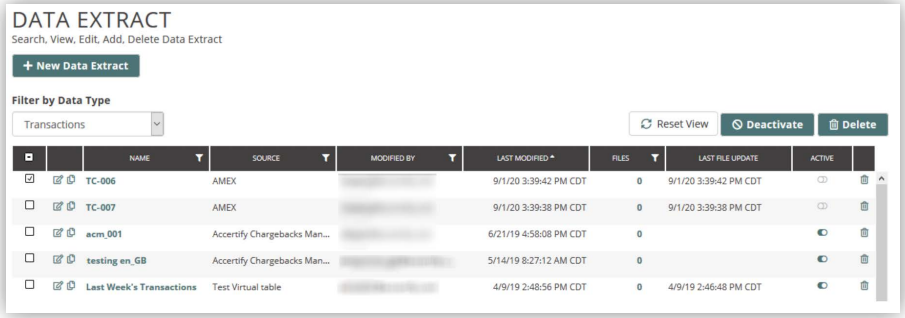


Accertify, Inc.

- **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 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.



Account Protection

In the last few years alone, billions of email addresses, passwords, and other personally identifiable information has been exposed on the dark web. As a result, criminals have harvested this data to execute sophisticated attacks designed to take over existing accounts or fraudulently open new ones. These acts are estimated to cost US firms over $5B annually[1].

To combat these problems, many businesses utilize several solutions to help prevent fraud, reduce loss, and enhance the customer experience. However, juggling multiple vendors can be costly, can present a fragmented risk picture, and can introduce unwelcome friction for your best customers.

With a constantly evolving threat landscape, it is imperative for businesses to partner with a company that provides an end-to-end solution across the entire customer journey.

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

Accertify, Inc.

Account Protection monitors customer activity in environments with a focus on identifying risk associated with Account Takeovers and New Account Openings. The product can detect loyalty theft, bots, credential stuffing, promotional abuse, card testing, and fake marketplace sellers.

Main Use Cases

Account Creation

Multi-Accounting
- Promo Abuse
- Free Trial Abuse
- Products on Credit

Marketplace
- Fake Sellers
- Fake Buyers
- Fake Reviews

Triangulation
- Sign Up on Behalf of Customer

Login

Credential Stuffing

ATOs

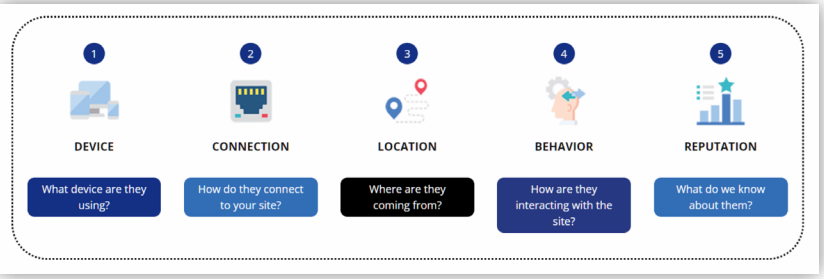
Account Update

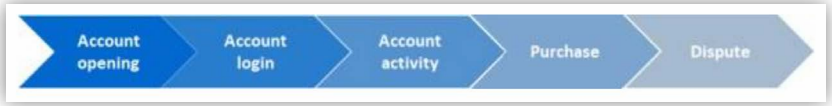
Card Testing/Wallet
- Loading Multiple Cards
- Card Tumbling

Loyalty Theft
- Redeeming Points on Account
- Transfer
- Third Party Redemption

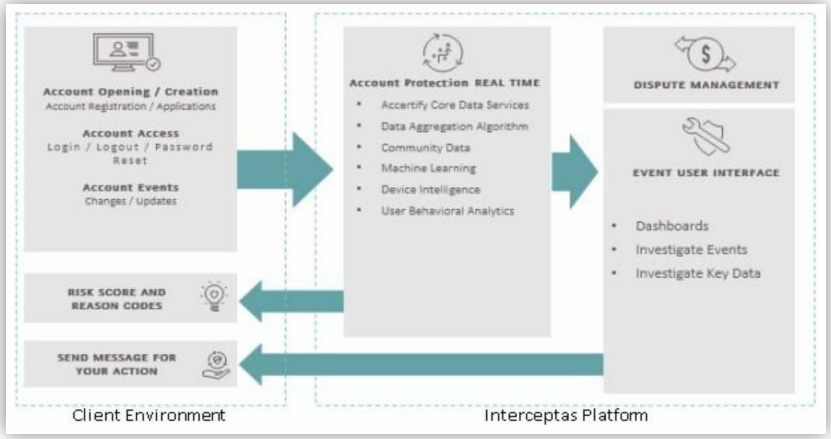
From the moment a customer enters the digital environment, Account Protection works in a frictionless way to provide real-time end-to-end insight, distinguishing good from bad activity.

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





The Account Protection Management Module monitors for fraud before, during, and after a purchase. Account Protection combines continuous monitoring and machine-learning algorithms to identify risky event activity when an event occurs, so clients can respond in real time. In addition, Account Protection provides a user interface, which allows clients to investigate suspicious activity and respond as they see fit.

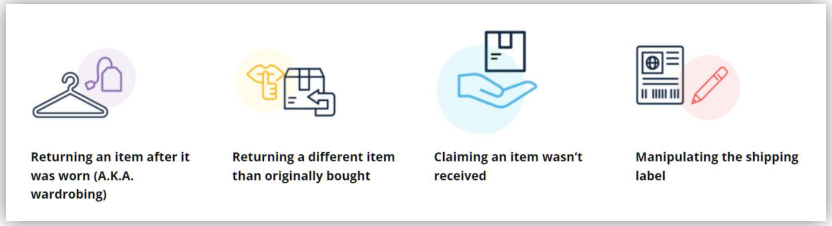


Account Protection monitors data and behaviors in the user environment and returns with a risk assessment and when a new event triggers, uses the newly collected data and compares it against historic data to analyze for consistency and anomalies.

While a user is browsing, we are collecting data such as user behavior analytics, device fingerprint, operating system, geolocation, and more.

CARE (Claims, Adjustments, Returns, and Exchanges)

Many returns are legitimate, but when done excessively, the costs can add up—resulting in a customer becoming unprofitable. There are also customers who knowingly perform malicious returns and profit from back-office processing problems or policy loopholes.

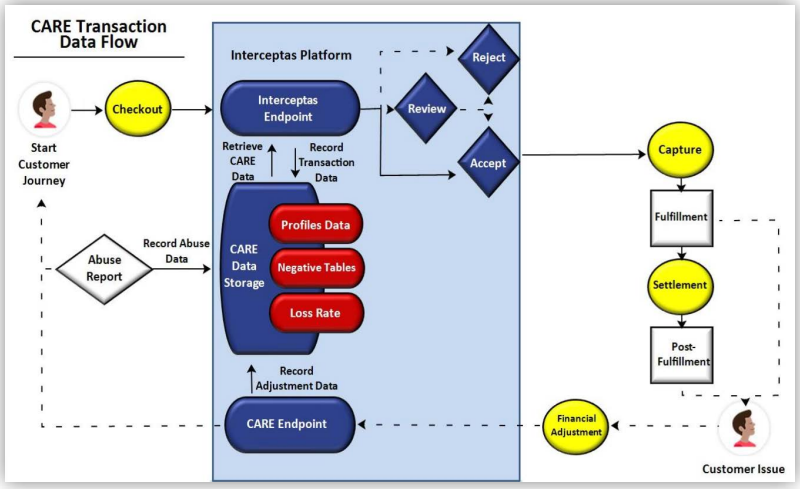


Many merchants lack the data needed to identify those who exploit their return policies or those who make legitimate but excessive returns. To address these growing problems, retailers need a solution to help prevent abuse without impacting the experience for good customers.

CARE is a purpose-built solution that collects customers' return data and allows merchants to monitor, measure, and take appropriate action in real time or to prevent future returns abuse. The CARE solution expands the capacity of the Interceptas® Data Management Platform to identify risks associated with Post-Fulfillment Adjustments, which are claims, adjustments, refunds, returns, reshipping, and exchanges. CARE provides current Interceptas Platform users with a dedicated API and a unique endpoint to send Post-Fulfillment Adjustments to transactions previously imported by the Interceptas Platform.

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

Process Flow



Refund Abuse Prevention

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

The Refunds Module is designed to identify and prevent patterns of claims abuse. The solution directly addresses the problem without causing unnecessary friction for trusted shoppers.

Through an easy-to-implement API, this dynamic, risk-based approach allows clients to accurately discern whether a refund claim is legitimate or fraudulent and take the appropriate action. By introducing a standard, risk-based technology approach that considers many different variables, merchants can now effectively begin to measure and monitor a previously undefined process.

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

Merchants report a growing issue of people returning items that are different from what they originally purchased, such as clothes worn once and returned, or a less-expensive item being returned instead of a more expensive one purchased, or even returning empty boxes. This is an operational issue and involves the warehouse teams that receive the package, so it is imperative they are communicating with the other teams across the organization when this happens.

Other Accertify Services Offered:

Decision Sciences: Accertify's global team of machine-learning experts and data scientists build industry-leading machine learning models, backed by **Accertify's** unparalleled network of reputational community data. These models provide clear, defensible reason codes that detail insight into the factors driving the model decision.

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

Client Success Management (CSM): The global team of Client Success Managers are responsible for assisting each client in achieving their fraud and chargeback goals. This team is primarily composed of former Directors and Managers of Fraud for the most recognized brands in the world and possess extensive first-hand fraud and chargeback experience. Client Success Managers have a deep understanding of the **Accertify** Fraud

and Chargeback Platform and understand how it can be deployed to solve complex challenges. The team stays closely aligned internally to ensure clients are aware of new features and functionalities.

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

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

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

ACI Worldwide (ACI Fraud Management)

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

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

In an era where identity-based fraud is prevalent, understanding each digital identity in real-time becomes critical. **ACI** addresses this challenge by developing precise strategies for rapid scalability and evolution. Their goal is to optimize the consumer experience, eliminate biases, and facilitate payment acceptance across diverse methods, channels, and geographies.

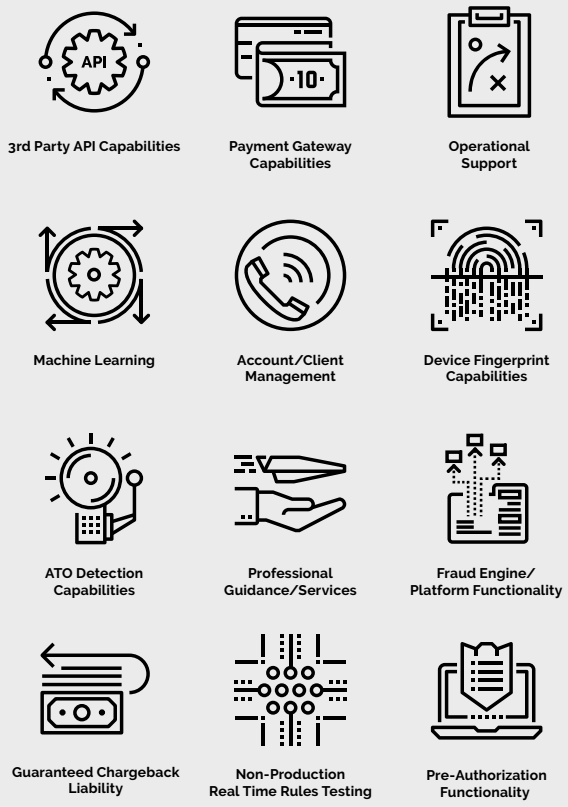
How does **ACI** achieve this? Through Payments Intelligence—an approach that leverages patented incremental machine learning models and proprietary network intelligence. By analyzing over 225 billion transactions annually, **ACI** supports organizations in automating processes and staying ahead in the dynamic payments and fraud landscape.

ACI Worldwide is committed to innovation and precision. **ACI** is proud to support over 80,000 merchants (directly and indirectly) as well as serving the top 10 banks and securing the ecosystem of over 1,500 banks and intermediaries.

ACI understands the challenge of balancing consumer convenience with security. As the industry undergoes a rapid AI transformation, **ACI** is at the forefront of innovation,

ACI Worldwide
Real-Time Payments

At a Glance:



with its patented incremental machine learning technology and synchronously running models to understand both digital identities and behaviors, supporting organizations to minimize operational costs and generate trust with their customers – all monitored and optimized by **ACI** patented AI models. Payments Intelligence supports understanding the consumers' digital identities and their preferences and building longer, lasting relationships – helping organizations to deliver hyper-personalized journeys.

For banks and financial institutions, **ACI** focuses on identifying good customers and this translates into the ability to deliver on reduced false-positive ratios, offer better customer experience (for corporate as well as personal accounts), and minimize operational costs by consolidating the overall fraud management processes. Governed by unbiased AI models, **ACI** access intelligence and delivers precise actionable intelligence in real-time without hampering a financial institution's credibility and revenue.

ACI Payments Intelligence for Banks and Intermediaries

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

As artificial intelligence (AI) adoption increases in the form of sophisticated risk threats, **ACI's** solution accelerates time to value for AI-driven solutions, providing a secure and transparent environment for consumers to transact. With nearly three decades of delivering AI-powered solutions, **ACI** has helped organizations boost their operational efficiency, mitigate risks, and power an enriched payment experience.

ACI's solutions constantly monitor a financial institution's account relationship and the transaction and non-financial event journey agnostic of the channel, method and geography, including holistic consumer behaviors. The ability to support each relationship lifecycle continuum with precise and actionable insights has enabled **ACI** customers to focus on essential business outcomes – without compromising on precision or transparency.

ACI further powers anti-financial crime action globally for over 1,500 financial institutions, representing the **ACI** flagship solution for contextual risk analysis and decision-making for authorized and unauthorized transactions and delivering against increasing regulatory and customer demand.

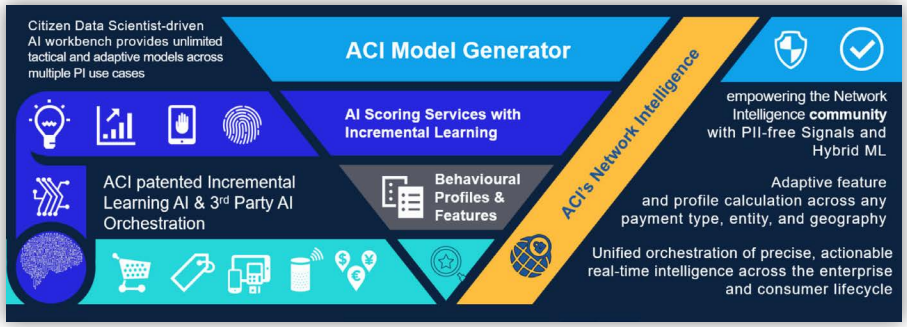
ACI Worldwide (ACI Fraud Management)

With the vision of empowering a secure payment ecosystem, **ACI** provides a choice of deployment options: from on-premise, on-demand, to public or private cloud with a subscription-based plan. **ACI's** solution is scalable, agile, and unbiased. **ACI** provides, manages, and implements a client solution in Azure, allowing organizations to focus on the business of fighting fraud.

With data orchestration elements, banks and financial institutions can take control of scams, cards, digital channels, and/or AML strategies, with screening flexibility for watchlist management or any identity provider in the world. **ACI** has an extensive range of partners to bolster the solution. Customers can implement SMS fraud alerts to combat scams and provide frictionless protection.

ACI offers a wide range of machine learning options depending on customers' needs, plACIng AI capabilities directly into the hands of fraud teams:

- **Fraud scoring services,** Stay ahead of fraud with effortless, real-time, fully managed, automated fraud scoring services driven by **ACI's** patented incremental learning capabilities deployed in the Microsoft Azure public cloud via an API.
- **ACI Model Generator, Democratized machine learning,** or make intelligence accessible to all, by taking full control of adaptive machine learning models and deploying them within hours.
- **Network Intelligence, (ACI's proprietary) Federated Machine Learning. Distribute,** exchange, and consume risk signals. **ACI's** proprietary network intelligence technology allows banks, processors, acquirers, and networks to securely share industry-wide fraud signals to feed their machine-learning models alongside proprietary data.



For Merchants

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

ACI Worldwide (ACI Fraud Management)

ACI's digital identity services has the ability to detect, orchestrate, and utilize over 10,000 data features from multiple data sources that enable a consumer's digital identity to be validated. Digital Identity Services enables automated decisioning to optimize revenue by reducing manual or human intervention. It is fully integrated into the payment flow via a single API, enabling both pre- and post-auth workflow screening and flexible strategies across channels, payment types, and regions. This, along with high-performance metrics and active/active architecture, gives the customer the scalability and flexibility to optimize accept/reject decisions – in real-time.

As mentioned above, with the constant threat of synthetic identity and ATO behaviors merchants regularly risk of losing revenue and reputation, **ACI** is able to deploy patented incremental AI models, capable of running in sync and tackling different challenges that could lead to eroding trust and margins.

Features include:

Precise performance: Transactional intelligence across verticals/industry sectors is leveraged to ensure a fraud-free environment and reduce false positives to a leading 3:1 ratio.

Performance guarantee: Merchants are assured that a minimum baseline will be achieved across conversions vs false positives, fraud, and cost of fraud.

Reduce fraud and chargebacks: Reduce chargebacks and false positives to increase profitability and conversion rates.

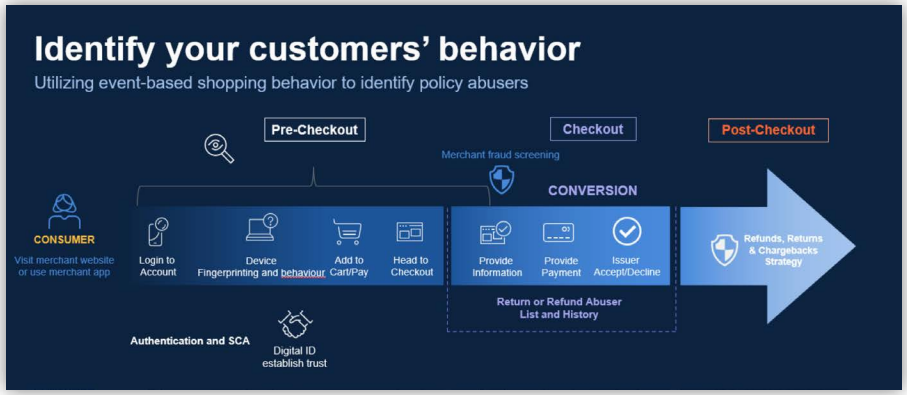
Minimize fraud-related operational cost: Streamline systems and remove complexities.

Improve customer experience: Deliver customer-centric buying experiences backed by holistic real-time fraud prevention.

Scalable fraud prevention: Give access to more features and functionalities, fully embedded in the payment flow.

With access to **ACI** Payments Intelligence technology and orchestration abilities, **ACI** also provides its customers access to an entire payments orchestration platform, capable of accepting transactions across any method, channel, geography, agnostic of industry sectors and nature of business. **ACI** Payment Intelligence can also be integrated via one of the company's many intermediary partners, including PSPs, acquirers, marketplaces, and systems integrators.

ACI Payments Intelligence: Achieving Precise, Actionable Intelligence in Real-Time



Data Richness

- **Digital Identity Services: ACI** helps organizations address an increase in bad data acquired through the use of stolen credentials used to create synthetic IDs and bots. This is achieved by reviewing transactional data from the merchant and then screening against multiple tools and technologies. This makes possible a positive or negative profile of the consumer's digital identity—and the likelihood of risk.
- **Behavioral Analytics:** It allows visibility into the pre-checkout browsing behavior of the consumer, helping to assess navigational behaviors and score the risk. This score is absorbed into **ACI's** core fraud strategy and is used to influence the final automated decision.
- **Incrementally learning AI Models:** Traditional machine learning can lack the rapid adaptability and transparency merchants need for successful fraud management. **ACI's** patented incremental learning algorithm solves the problem of costly and time-consuming model performance degradation and allows machine learning models to adjust to new behaviors without the need to re-learn everything they already know.

This means that new data is input to the models on a daily basis and new behaviors can be identified in near real-time. In this model, machine learning performance lasts for longer, without degradation. It also removes the need for costly and time-consuming model refreshes. **ACI's** machine learning models are supported by a dedicated team of data scientists. Model options include:

- Custom models
- Merchant-specific models (for larger merchants)
- Over 15 vertical-focused models (including telco, travel, retail, gaming, and digital)

Over 7,500 AI features are used to create ACI models, ensuring high performance regardless of sector.

- **Advanced behavioral profiling:** The power of profiling lies in the combination of sophisticated analytics with cross-sector merchant network data, machine learning, and flexible fraud prevention tools. Positive and negative profiling calculations

make fraud event detection and prevention more accurate, and they vastly reduce false positives, which translates to converting (accepting) more transactions and reducing costs associated with false positives.

By analyzing the history of transactional data across all **ACI** merchants, positive profiling can match over 10,000 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.

- **Third-party callouts:** One integration gives merchants access to several third-party providers whereby the returned fraud score can be utilized within the core fraud strategy at ACI. ACI fACIlitates the call to the service, based on configurable qualifying data points in both real-time or near-real-time using via decision flows.
- **Link analysis:** This analysis identifies data points associated with a confirmed fraudulent data point, allowing visibility into patterns of emerging fraudulent behavior.
- **Autopilot:** This monitors real-time responses and automatically blocks associated order elements based on high-efficiency strategies or features for a specific period.
- **Auto-Analyst:** 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 scale rapidly 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 for "buy now/pick up in store" orders.
- **Third-party orchestration:** One integration and one contract with **ACI** gives merchants access to several third-party providers; they can call the service based on configurable data points in both real-time or near real-time processing steps or decision flows.

  To manage costs, **ACI** utilizes smart routing functionality so transactions can be qualified in or out for third-party callouts. **ACI** can automate connectivity and receive responses in real-time and post-real-time to incorporate into the overall core strategy and influence final decisions.
- **Weighted scoring: ACI** can provide weighted scoring and prioritization to the multi-layered components within the fraud strategy. By individually weighing the priority of scores, e.g. ranking the importance of specific checks, strategies, and validations over others, **ACI** ensures that acceptance rates are optimized but costly false positives and fraud are minimized. The cumulative weighted scores can then be totaled and will ultimately determine the outcome of the overall automated decision.

  Scores and weightings are regularly reviewed and can be amended as required to ensure optimization. **ACI's** team of Data Scientists and payment optimization specialists will work

with the client to agree on weighting plans. This approach allows clients to determine how much the model influences the overall decision, allowing for a machine-learning-first approach or a hybrid one depending on preference.

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

Processes

- **Case Manager:** This workflow management tool allows prioritization of workflows (such as order value and delivery channel).
- **Smart Dynamic Routing:** To manage costs, **ACI** utilizes smart routing functionality so transactions can be qualified in or out for third-party callouts. **ACI** can automate connectivity and receive responses in real-time and post real-time to incorporate them into the overall core strategy and influence final decisions.
- **Robotic Process Automation:** This enables business automation for organizations by leveraging intelligence to respond to flags and alerts, reduces human involvement, and enables a seamless customer journey to complete their transaction – increasing process velocity.

Performance

- **Silent mode for A/B strategy testing:** This can be applied to run in parallel through silent mode for a period before applying to active mode (production), such as in champion/challenger strategies. This allows merchants to test the effectiveness of a strategy and optimize it without impacting live customer transactions.
- **Enhanced response:** Additional information is provided, such as the reason for the response given alongside additional response metadata detailing the elements that contributed

to the result. This can be incorporated into a merchant's (or partner's/PSP's) own user interface and internal platforms.

Expert consultancy and human intelligence

- **ACI Consultancy for banking: ACI's** consultancy provides the operational, analytical, and technical expertise fraud management teams need to make the most of their technology investments. They offer custom-tailored, optimized rulesets and services to ensure strategies are effective, and they optimize configurations and workflows to ensure cost-effectiveness. Consultants are based all around the world with geographically and culturally relevant fraud expertise.
- **Payments Strategy and Optimization Specialists for merchants: ACI's** global team of dedicated specialists spans 4 continents (and 15 languages) and has access to global payments intelligence and local market knowledge. They have an average of five years of experience, and many are certified e-commerce fraud professionals. 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.
- **Manual order review for merchants:** Merchants are provided a team of analysts to validate and authenticate challenged transactions for a final decision. Decisioning accuracy is tracked and monitored to ensure key performance indicators are met, averaging a 99.99% rate. Service can be deployed during season peak periods, weekends, or daily.
- **Data Scientists for both banking and merchants: ACI's** dedicated team of data scientists brings decades of experience and expertise. The team is responsible for both AI and machine-learning strategies across the payments ecosystem. They have over 15 consortium models in production, covering all main verticals from retail to clothing, gaming, and travel. The team continues to innovate, bringing new technology to market, preventing fraud, and helping customers utilize machine learning in a meaningful way. The team is multilingual, with representation in the US and Europe. Academically, the team is well-published, with over 30 publications between them, continuing to contribute to the ever-evolving domain of data science.
- Human Intelligence plays a crucial role in controlling AI models and strategies. Our Human intelligence can detect flaws, biases, or unintended consequences in AI models, providing provide valuable insights to improve and adjust the models over time. Through continuous human intervention, AI systems can evolve and ensure that they improve and optimize accuracy and efficiency and manage false positives
- **HELP24 Support for banking and merchants:** 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)

Integration Process

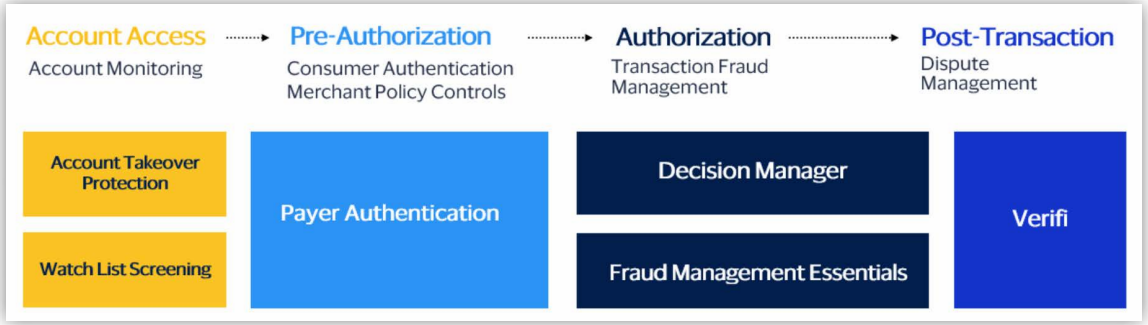
ACI offers merchants a cloud-based deployment for its e-commerce fraud capabilities. Integration can range from a couple of days to a couple of weeks, depending on the size of the implementation. It can be accomplished with a simple API integration.

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 a historical data submission from the client (if available) using at least six months of data on 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.

Cybersource

Cybersource, a vital pillar of the Visa Acceptance Solutions family, provides a cutting-edge combination of automation and customization for exceptional control over both fraud and revenue, with reliability and security of **Visa**.

The comprehensive defense offered by **Cybersource's** suite of risk products continuously increases revenue thanks to AI. The machine learning at the core of the fraud management product suite constantly improves and optimizes thanks to the billions of transactions running through both the **Visa** and **Cybersource** networks.



Core Capabilities

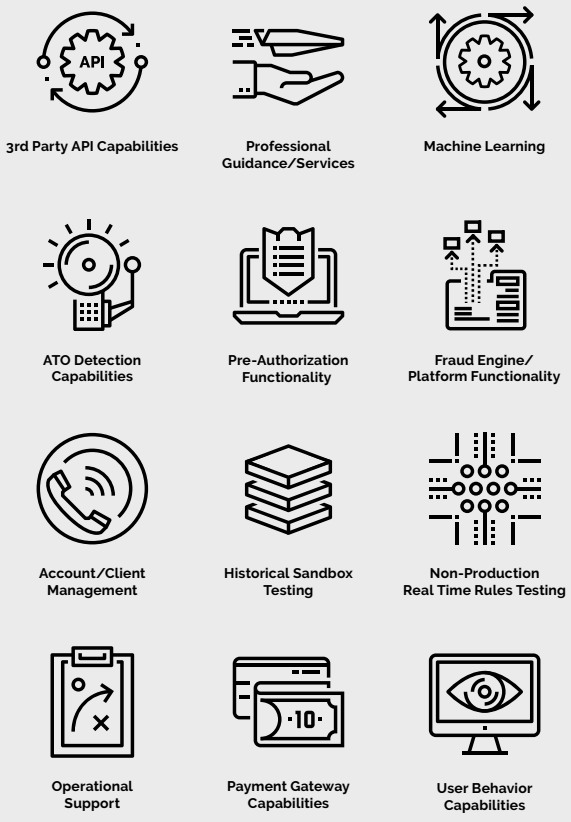
At the heart of **Cybersource** is a modular, cloud-based platform. Using a single set of APIs, **Cybersource** can integrate with any system in the market and support any vertical, including: retail, ecommerce, transit, telecommunications, restaurants, airlines, insurance, and utilities configured to solve beyond merchant fraud and traditional industries.

The **Cybersource** and **Visa** ecosystem provides 276.3 billion transactions per year[1] of insights. Each one provides insights to help optimize fraud prevention, capture more

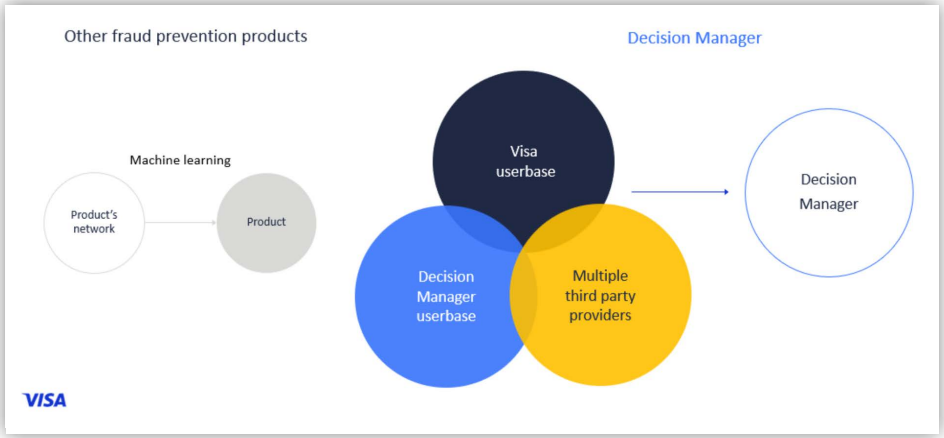
[1] https://usa.visa.com/dam/VCOM/global/about-visa/documents/aboutvisafactsheet.pdf

cybersource
A Visa Solution

At a Glance:



revenue, and improve authorization rates. Its systems are built on proven **Visa** systems, so data is secure.



Automate your fraud decisions with AI

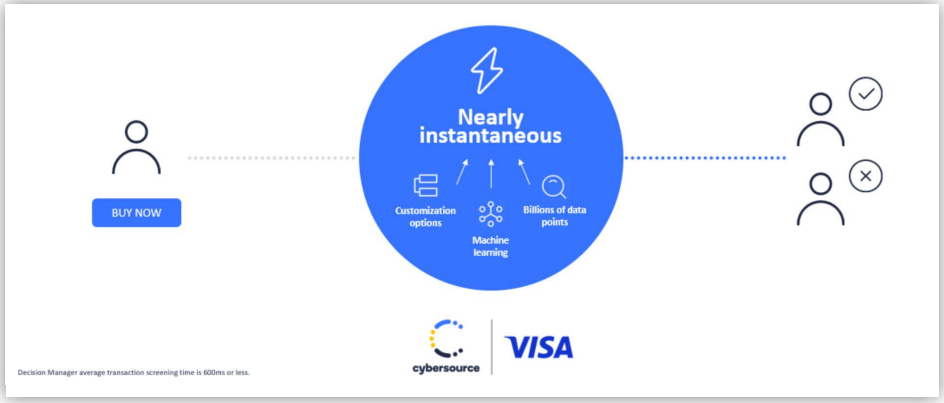
- Advanced AI resolves 99.3% of Decision Manager transactions and continues to migrate more and more clients toward full automation.[2]

Shift the focus to accepting more good customers

- The innovative AI-powered Identity Behavior Analysis proactively enables business with the 99% of transactions that are valid.[3]
- It can improve decisions and help avoid false positives. It also helps provide a better customer experience for good customers who don't have to be screened for fraud.

Make lightning-fast decisions

When a customer makes a purchase, Decision Manager's customization options, machine learning, and billions of data points come together nearly instantaneously to determine the validity of the transaction. Without waiting or status timers, instant decisions drive a smoother customer experience.



Increase revenue, decrease fraud

Decision Manager

Powered by machine learning, Decision Manager can improve authorization and increase revenue, not just prevent fraud, all to help improve customer experience. With deep customization options and a robust reporting suite, Decision Manager is ideal for enterprise clients who desire refined control over their sales and fraud strategies.

[2] September, 2023 results measured as a rate of total Decision Manager transactions from Visa
[3] Measured across all Decision Manager transactions in July, 2022

Cybersource

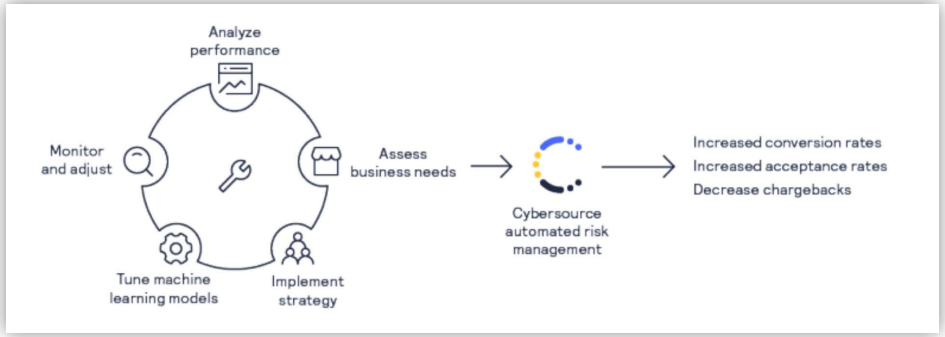
As a fraud prevention and risk management tool, Decision Manager allows businesses to accept or reject incoming transactions based on learnings from **Visa**, **Cybersource**, and other third-party data providers. It comes fully integrated with payment management or is available as a standalone service.

Combined with decades of fraud management and data science experience, this unparalleled scale allows **Cybersource** to deliver accurate, automated risk scores that help businesses produce real results.

Revenue Optimization Solution

Cybersource's Revenue Optimization Solution is for businesses who prefer to outsource and automate fraud management. It balances a fraud strategy with seamless payment acceptance for good customers. As an all-in-one hands-off solution, it seamlessly balances identity verification, fraud strategy, and payment acceptance to ensure your business is secure.

When businesses entrust their fraud management to **Cybersource**, they're assured a fraud chargeback rate and a Decision Manager acceptance rate that aligns with the business's goals, increases revenue, and reduces customer friction. Businesses that outsourced risk management to **Cybersource** saved $4 million in manual review costs and increased acceptance revenue by $36.8 million in 2021.[4]



Fraud Management Essentials

Fraud Management Essentials is the small and midmarket fraud solution of choice. With ready-to-go fraud filters, businesses can automatically monitor transactions while still providing a seamless customer experience. It's a streamlined and powerful fraud prevention tool to prevent common fraud attacks such as card testing, payment fraud, and common abuse scenarios. Built on the same machine learning network as Decision Manager, Fraud Management Essentials utilizes powerful risk models and hundreds of validation tests to automate detection and prevent fraudulent transactions.

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

[4] Results calculated using internal data based on Decision Manager clients in North America during January 2020 to November 2021. Results will vary based on factors including if client works with Cybersource Managed Risk

A complete suite of solutions

Machine Learning

Based on more than 276 billion transactions annually[5], **Cybersource's** artificial intelligence engine consists of multiple constantly-evolving neural networks interlocked to assess active behaviors without the need for manual intervention.

Network

Unparalleled uptime and stability along with the global reach of all Visa and Decision Manager transactions.

Identity Behavior Analysis

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

Customization

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

Digital Device Identity

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

Transparent Decisions

Cybersource's risk products offer full insight into the reasons why a decision was made, not just the decision. Tools such as Decision Manager Replay create a safe zone for clients to review and test new strategies without impacting customer experience.

Reporting

A range of dashboards and reports complement comprehensive custom reporting options.

Third-Party Data Providers

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

Account Takeover Protection

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

Watch List Screening

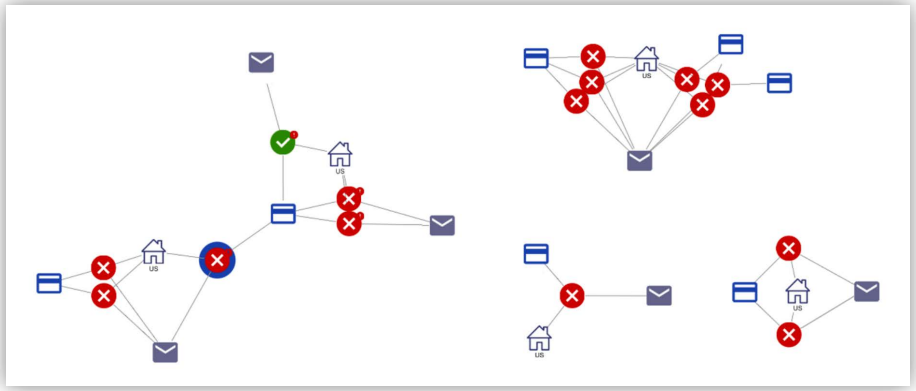
Watch List Screening offers real-time screening to global sanctioned and denied parties lists. This provides knowledge to make informed

[5] Machine learning algorithm is based on Visa transactions (276B) + Decision Manager transactions + third-party data partners' transactions

decisions about denied parties, even to businesses not required to connect to these lists by regulation.

Transaction Management
Direct access to review and investigate individual transactions.

Expertise
Cybersource's fraud solutions are supported by experts on the cutting edge of fraud, and merchants can choose to work with a Risk Solutions Services Consultant for personal expertise and support.



Discover the links between positive and negative transactions with Decision Manager's visualization options.

Merchant Experience

Cybersource's end-to-end solutions, within a single platform, empower merchants to focus their attention where it matters most. Merchants can utilize **Cybersource's** solutions to solve a wide array of business problems, all while preventing fraud.

Risk Solutions Services
Merchants benefit from **Cybersource's** powerful automation tools and can strike a balance between automation and experience by leveraging smart humans.

With highly experienced consultants around the globe, Managed Risk Services provides businesses with the expert in-person support that can make such a difference when managing fraud strategies.

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

Pricing Model

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

Planned Updates and Enhancements

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

Case studies, comparisons, statistics, research, and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Cybersource neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required.

Experian

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

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

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

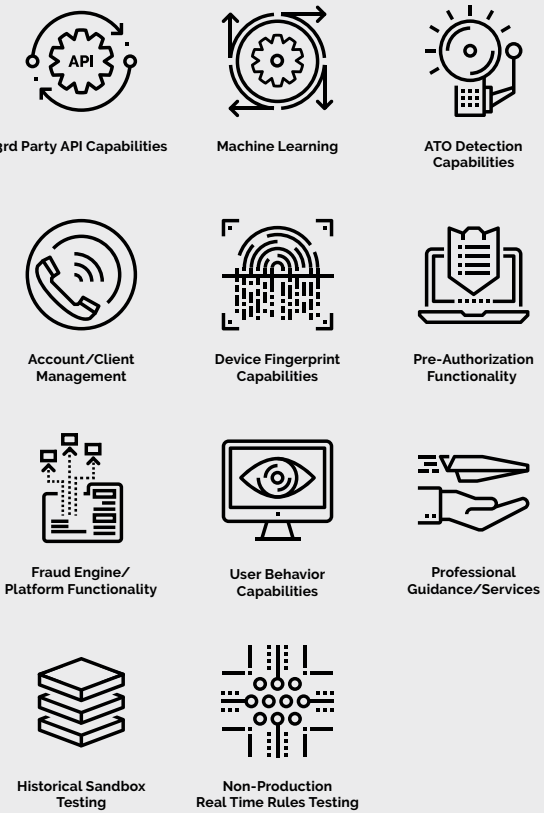
Experian Identity and Fraud solutions focus on five primary client needs:

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

Solutions and Functionality:

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

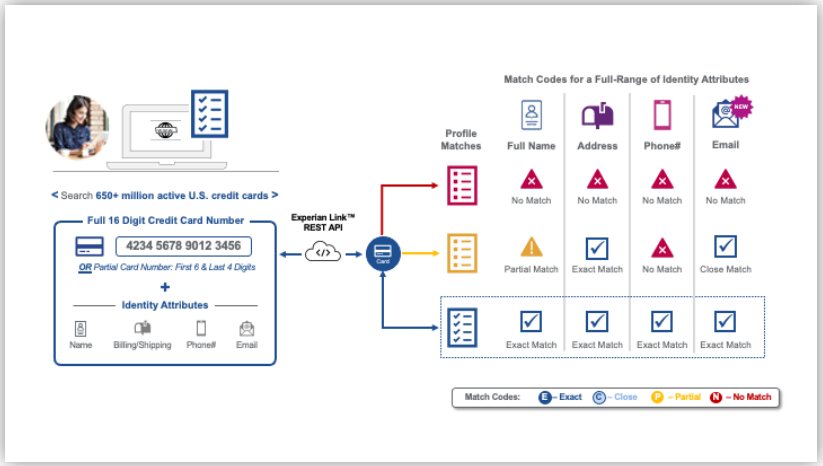
At a Glance:



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

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

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



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

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

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

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

Reporting options available:

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

Proof of Concept process:

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

Pricing format:

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

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

Integration options available:

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

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

White-label options are available, and third-party integration partners include loan origination, payments, and other providers.

Backing partners deliver niche capabilities that include email intelligence, phone intelligence, behavioral biometrics, alternative consumer information, document verification, and international consumer data.

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

Available Support:

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

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

Continued enhancement to identity resolution and fraud predictiveness through additional data sources (internal and external), coupled with advancements in analytics around machine learning, AI, attributes, and triggers. This includes giving clients access to data and attributes in a self-service sandbox, creating signals, and enhancing fraud detection capabilities to reduce false positives and drive better customer experiences and outcomes.

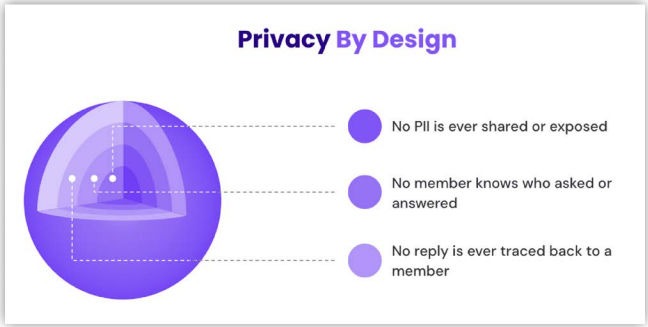
Authentication enhancements provide clients with an increased number of choices to meet business needs. This includes an emphasis on more passive tools like behavioral analytics and continued enhancements to present appropriate amounts of friction, such as document capture. For **Experian** Link, enhancements to PII component matching will include email and IP addresses as well as all-out scores for different combinations of PII.

Identity and fraud exchanges will help clients build consortiums to share data in a permissible manner and drive better fraud decisions, eliminating known bad actors as soon as possible from the ecosystem and reducing friction for good users.

Identiq

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

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



Each network member installs an "edge server" on-site. This is the cryptographic protocol based on secure multiparty computation, and includes a normalized database that remains in the member's environment at all times. Each member joins with all their data in order to participate in the validation of users against other members' databases. When a company queries the network, they send a one-time fully anonymous query to the other members

At a Glance:

- 3rd Party API Capabilities
- Historical Sandbox Testing
- Machine Learning
- Account/Client Management
- Pre-Authorization Functionality
- Fraud Engine/ Platform Functionality
- Non-Production Real Time Rules Testing

to ask if they already know and trust the customer. Based on the responses and degree of confidence, **Identiq** provides a score with sub-second response time.

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

Identiq clients leverage the network to achieve the following KPIs:

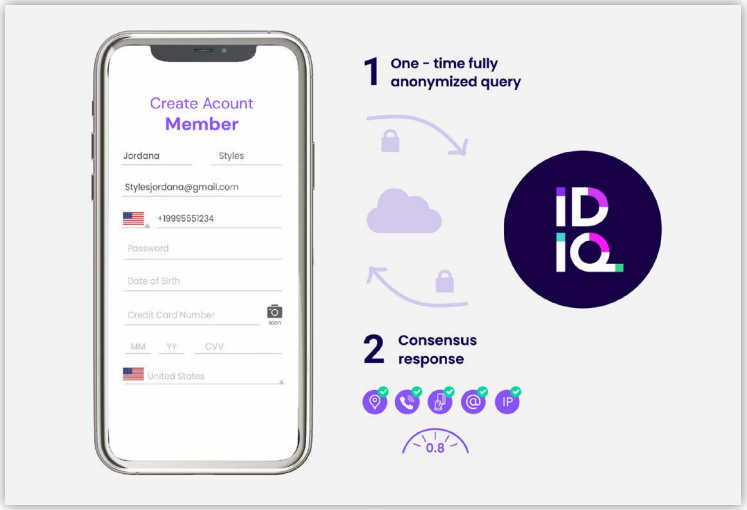
- Revenue increase
- False decline reduction
- Drop-off and friction reduction across different touchpoints throughout the customer journey
- Increased conversion rates and customer lifetime value
- Improving accuracy and performance of Machine Learning Models for risk assessment

Products and services

Identiq is a private network for identity validation that empowers companies to safely collaborate with each other in order to validate trusted customers without sharing any sensitive data or identifiable information. The peer-to-peer technology helps some of the world's largest companies to identify good customers, fight fraud, and offer better experiences throughout the digital journey.

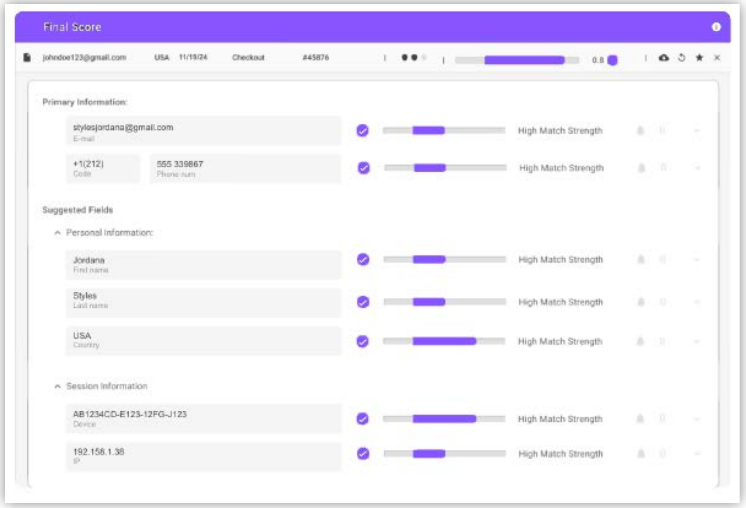
The main offerings include:

- **Decline Reduction:** Through the network, members can make more accurate decisions during transactions to increase payment approvals, reduce declines and friction, and maintain low fraud rates.
- **Sign-up Validation:** Member ecosystems are better protected by validating new customers at account creation. Trustworthy customers are let in with less friction and better experiences, while fraud is filtered out.



- **Risk-based Onboarding:** The network helps reduce the friction and dropoffs in KYC processes by identifying which customers can be trusted automatically and which cannot, resulting in accurate prioritization and cost reduction. This is also used

when a significant data point is changed, which can affect the trust or risk of the customer.



The **Identiq** network is secure and private by design and provides:

- **End user anonymity:** No consumer information is ever shared, exposed, or leaves the member's domain
- **Requester anonymity:** No other member can discover who is sending a query to the network
- **Voucher anonymity:** No member, including the one who made the query, can discover who is answering
- **No response disclosure:** No members can ever discover who was asked about or if they replied positively or negatively

Reporting options available

Identiq offers reports that include query and scoring data over time. However, the majority of network members integrate these reports into their custom reporting and tracking systems.

Proof-of-concept process

Two types of POCs:

- **Offline POC analysis that utilizes historical data.** As part of this POC, **Identiq** offers a Point-in-Time evaluation.
- **Live POC, which offers the highest accuracy of results.** Through this option, **Identiq** mimics the environment with a fully integrated live evaluation.

Pricing format

Pricing is based on a flat fee per query, regardless of the value of the transaction. Volume discounts are available which provide a greater economy of scale. In addition, the unique aspects of the private network include the data contribution element in the pricing structure. The more data a network member onboards onto the network, which provides tangible value to all members, the larger the discount from the list price will be.

Integration options available:
Direct API integration is available, as well as integration through a number of orchestration platforms. Elapsed time from signature to launch can range from 4-8 weeks.

Onboarding the **Identiq** network requires a three-part integration process:

1. Simple API integration
2. Installing the **Identiq** Edge–the cryptographic protocol–in the member's environment. If a member uses leading cloud providers, the required effort for installation is significantly reduced
3. Onboarding data onto the network, which is a data task more than an integration effort

Every member onboards with 100% of their data accessible to the network–which remains private at all times–leading to strong global coverage, including in regions where other vendors typically do not have a strong presence. **Identiq** works primarily with very large enterprises and with each new member, coverage grows exponentially. While Identiq is not a rule-based solution, the signals can be used by network members in any rule-based system.

Client support options
Every network member works with a dedicated account manager who works closely with them providing ongoing support and quarterly business reviews. When needed, members are provided with onsite visits and integration support.

12 month roadmap

With the proliferation of "friendly fraud" and the abilities generative AI now offers fraudsters of all levels, **Identiq's** key developments are focused on maintaining and enhancing a strong network where trust and risk can quickly be identified to keep network members' environments and businesses safe and private. Specific developments include:

- Enhancing the quality and accuracy of the **Identiq** score
- Enriching the ability to identify friendly fraud cases
- Boosting performance to new levels
- Creating direct connections to payment gateways for feedback loops

Kount, An Equifax Company

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

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

Kount®
An Equifax Company

At a Glance:

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

Kount, An Equifax Company

Kount's advanced artificial intelligence, combined with the Digital Identity 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 Digital Identity 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 machine learning analyzes historical fraud data and is trained on **Kount's** Digital Identity Global Network, which includes billions of transactions from over 15 years of data in over 250 countries and territories, as well as more than 50 payment and card networks. Unlike other providers, which require a learning curve to understand the intricacies of a customer's business, **Kount's** AI/ML combination outlined above works for customers on day one. This means that from the moment the solution is implemented, customers can experience its benefits without the need for extensive onboarding or adoption periods.

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

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

- Payments fraud protection
- Account takeover protection
- Data on Demand, fueled by Snowflake, for actionable customer insights
- Chargeback Management, integrated with Verifi, A Visa Solution, and Ethoca, a Mastercard Solution, for managing fraudulent transactions, chargebacks, and disputes

Kount, An Equifax Company

Payments Fraud Protection

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

Kount provides its payment fraud protection customers access to the Digital Identity 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 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** analytics and reporting functionality, Datamart, enables reporting on the 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, expand new use cases, and expand sales channels.

Account Takeover

Kount's account takeover solution provides frictionless account creation experiences, prevention of malicious logins or account creations, protection against bad and questionable bots, and the personalization of customer experiences. **Kount** takes a multilayered approach to account protection: adaptive protection against account takeover attacks, policy customization to fine-tune protection, plus reporting and data presentation to uncover trends. Together, they can reduce false positives, enable customized user experiences, and reveal trends that enrich custom data to inform future policies.

In the protection layer, **Kount** 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 a step-up secure multi-factor authentication.

In the policy and customization layer, **Kount** customizes user experiences and can help reduce friction by identifying and

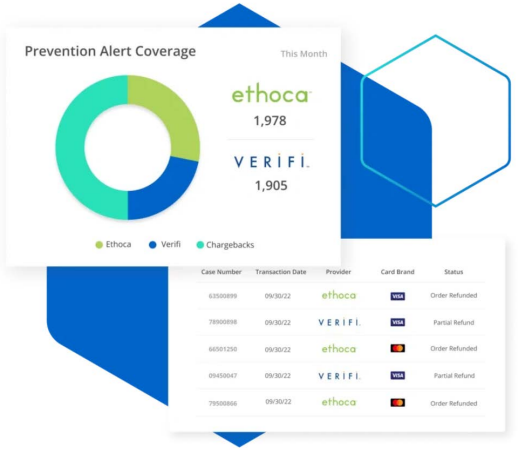
segmenting users based on common characteristics, such as VIP or trial users. **Kount** provides data such as user type, device specifics, IP risk, geolocation, and custom data.

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

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

Chargeback Management is a solution that can provide chargeback prevention and mitigation while also providing a mechanism to manage and fight disputes as they arise. **Kount** has integrated with Ethoca to provide Consumer Clarity™ and Ethoca Alerts. **Kount** is also integrated with Verifi and provides Order Insights, Compelling Evidence 3.0, Inform, RDR, and CDRN. Customers can take advantage of chargeback prevention tools to identify, prevent, and resolve chargebacks without the need for development resources or complex integrations. Chargeback Management delivers all of the benefits of **Kount's** fraud prevention plus the enhanced capabilities for Verifi and Ethoca's order validation, compelling evidence, and dispute management tools. Together they help stop chargeback losses and reduce dispute timeframes.



Partners

Customers can gain access to the Digital Identity 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, Fiserv, BlueSnap, and others. **Kount** also partners with ecommerce platforms and payment partners, such as Shopify, WooCommerce, Magento and BigCommerce among others.

Kount's partners access and manage fraud prevention for their merchants through an AI-driven fraud protection suite for online payment processors, payment gateways, hosted payment pages, and ecommerce platforms. **Kount** 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

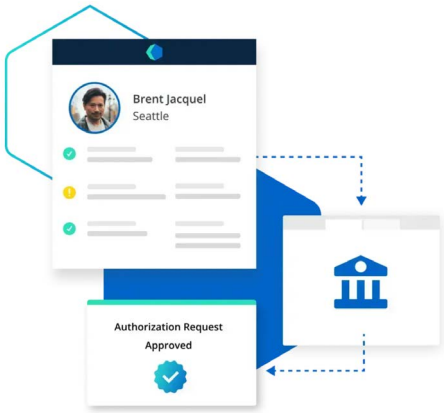
Kount customers can further enhance their fraud prevention strategies with features and functionality such as the following:

- 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 Digital Identity 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** Digital Identity Global Network's billions of data points, Email Insights informs identity trust with data on payments, location, and digital identifiers. In addition to



predicting a customer's level of trust, Email Insights can help businesses understand a customer's lifetime value and likelihood of making repeat purchases.

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

Kount 360

Kount 360 is a new integrated identity and payments platform, powered by the Equifax Cloud™, that integrates the full suite of **Kount** solutions and is delivered with a single API and user interface. **Kount** 360 helps merchants, financial institutions and other businesses prevent digital fraud and achieve operational efficiency by removing the need to manage multiple point solutions while also reducing dependency on third-party technology platforms and providers.

The **Kount** 360 platform harnesses the power of the **Equifax** Cloud and offers advanced capabilities to help businesses:

- **Combat new attack vectors,** such as address manipulation and cross-merchant card testing
- **Eliminate traditional account takeover fraud** while delivering passwordless authentication and reusable identities
- **Detect and prevent** Personal Identifiable Information (PII)-cycling card testing attacks in real time
- **Utilize optional pre-built decisioning models** for email insights, address verification, and more

Kount 360 will help to entrench the position of **Equifax** as an industry-leader in delivering advanced and differentiated payments, identity, and compliance solutions for businesses around the globe.

Professional Services

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

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

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

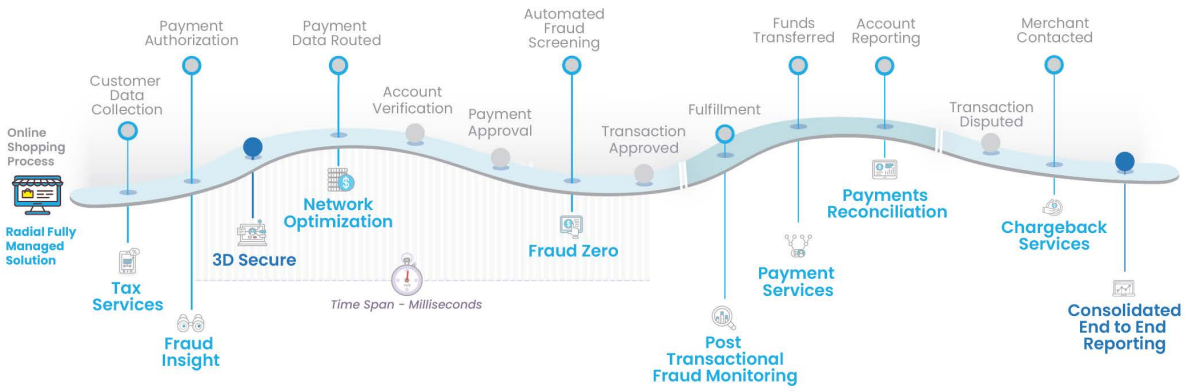
Kount's Consulting Services provide access to a broad team of fraud professionals with expertise across multiple industries and specialties. Businesses gain training for fraud analysts on manual review best practices, progress reporting, and expert guidance regarding control measures to implement throughout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

Radial

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

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



Radial
powering bpostgroup

At a Glance:

- 3rd Party API Capabilities
- Payment Gateway Capabilities
- Machine Learning
- Guaranteed Chargeback Liability
- ATO Detection Capabilities
- Account/Client Management
- Device Fingerprint Capabilities
- Historical Sandbox Testing
- Non-Production Real Time Rules Testing
- Pre-Authorization Functionality

RPS Fraud Services

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

Pre-Authorization: Fraud Insight

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

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

In addition to card testing and other common cases, **Fraud Insight** builds specific use cases from consortium data that can adjust to changing fraudulent tactics. **Fraud Insight** continuously monitors transaction flow and utilizes machine learning, large language model (LLM's), and proprietary data training sets to predict and implement more effective strategies.

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

Roadmap 2024

- Increasing behavioral data point types
- Adding alternative payment methods
- Adding ecommerce platform integrations

Post Authorization: Fraud Zero

RPS's Fraud Zero service is their comprehensive post-authorization product providing **fraud screening** to protect transactions after payment authorization. In developing the real-time fraud engine, they utilize various methods of machine learning, large language models, and proprietary data training sets to predict and implement more effective strategies. In

addition, their proprietary device-fingerprinting software contributes to a universal data profile that can then be utilized to rapidly determine customer identities and intent.

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

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

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

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

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

Roadmap 2024

- In-store integration for point-of-sale protection
- Additional application of LLMs
- Updating ecommerce platform integrations
- Social commerce integrations

RPS Processing Services

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

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

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

Processing Services includes the ability to remove any transmission of credit card data from a merchant's workflow. Beyond tokenization their secureform technology creates a secure channel of communication between the shopper's browser and **RPS** servers. This reduces the merchant PCI DSS scope to the lowest level possible for accepting ecommerce payments.

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

Roadmap 2024

- In-store integration of customer data platforms
- Additional alternative payment methods
- Updating ecommerce platform integrations
- Social commerce integrations

Chargeback Services

RPS' Managed Chargeback Services is a full service dispute management system organizations can use alone or integrated with RPS' Payment Processing or fraud solutions. **RPS** incorporates automation of chargeback notifications from processors, shipping details, and documentation from order management systems.

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

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

RPS monitors all network chargeback regulations and threshold requirements to keep clients informed of changes and actions that must be taken to be in compliance and provide guidance

on balancing checkout optimization with best practice recommendation on return policy and other terms and conditions.

Onboarding / Account Management

RPS' on-boarding begins with a consultative approach which tailors their their solution to adapt to your current situation and future plans. They have a dedicated team of payment, fraud, and chargeback specialists to assist in evaluating what solution would work best and how to prioritize options. For instance, depending on demographic and product risk profile, they may recommend that different Buy Now Pay Later solutions be added to a payment mix. For their Fraud Solution, **RPS** will provide a historical analysis of transactions to launch with an effective strategy starting on day one. The Managed Chargeback Services team will also review the clients current terms and conditions with the intent of suggesting changes to shape the objectives of the dispute strategy.

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

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

Pricing format

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

- Flat Fee
- Transaction based
- Payments — Pass through
- Fraud - % based on Cost Of Goods
- Chargebacks are included complimentary with a full Payments & Fraud Solution
- Fraud Solution can also be priced on a per-transaction fee

Riskified

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

Benefiting from a sizable team dedicated to researching global fraud and training machine learning models, the platform analyzes the individual behind each interaction to provide real-time decisions and robust identity-based insights. The platform reviews shoppers and transactions across its global merchant network, which processed approximately $120 billion in gross merchandise value (GMV) in 2023.

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

Solutions and Functionality:

Chargeback Guaranteed Fraud prevention:

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

riskified

At a Glance:

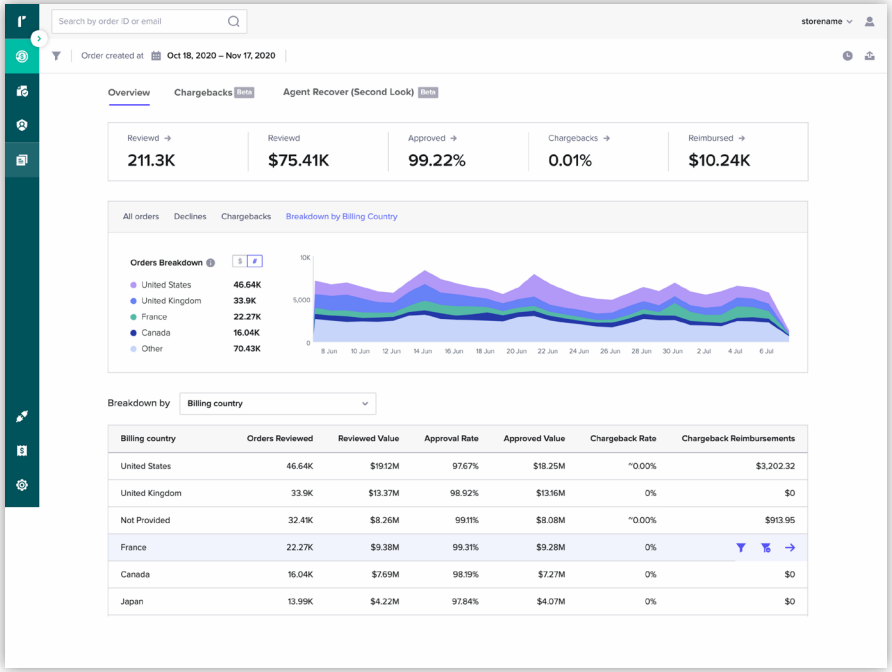
decision draws over on a billion prior transactions processed for global e-commerce organizations across industries.

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

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

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

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



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

Identity Explore, launched in 2023, enhances Policy Protect's capabilities by allowing merchants to visualize customer identities and behavior, tailor customer experience, and customize policy decisions. A high-resolution visualization of **Riskified's** identity

engine, Identity Explore gives merchants the ability to analyze, investigate, and interact with customers on a whole new level. Through this offering merchants are empowered to optimize, and ultimately personalize, their policies.

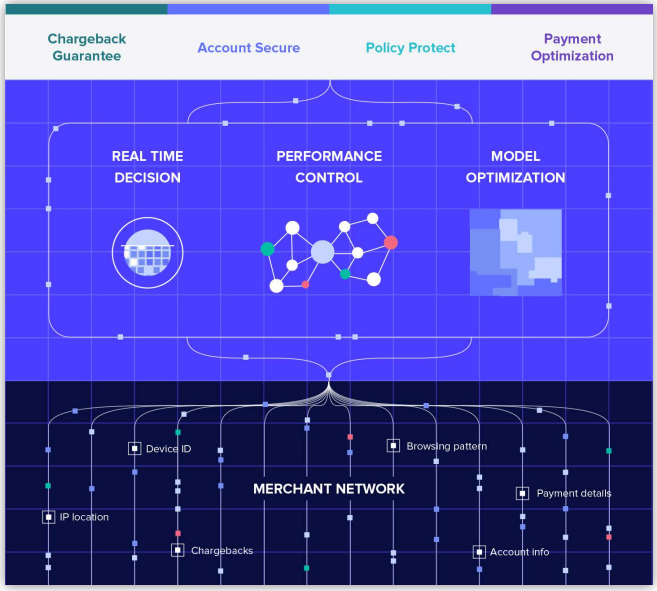
Dispute Resolve:
Dispute Resolve allows merchants to simplify their chargeback management operations with a single smart platform.

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

Chargeback workflows differ depending on what, where, and how you sell. Dispute Resolve can automate as much or as little as you desire, allowing you to maximize efficiency while retaining as much control as you need.

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

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

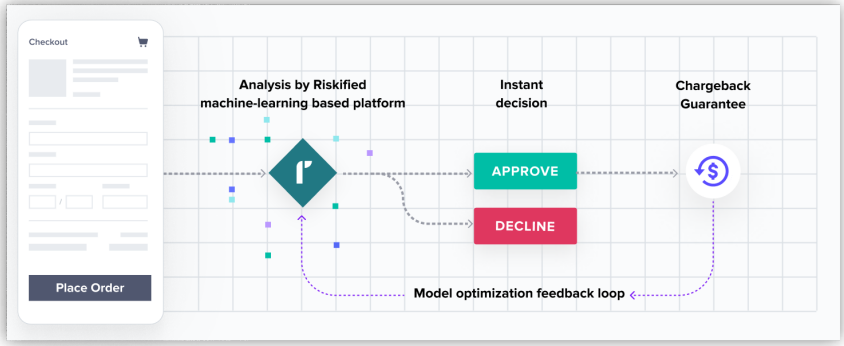


In addition to analyzing device and behavioral factors, Account Secure's accuracy is largely fueled by **Riskified's** expertise on the transaction level. Each login and account event is linked to historical transactions both at this merchant, and across their network.

Reporting options available:

Riskified Chargeback Reporting view provides aggregated chargeback reimbursement and dispute stats in the Control Center dashboard, and offers granular data so users can track

reimbursements and disputes on the order level. This allows merchants to easily track **Riskified's** performance and gain insights into chargeback populations. Users can analyze specific chargebacks and disputes when relevant.



Proof-of-Concept process:

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

Pricing Format:

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

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

Integration:

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

Riskified

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

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

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

Support packages available:

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

Sardine

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

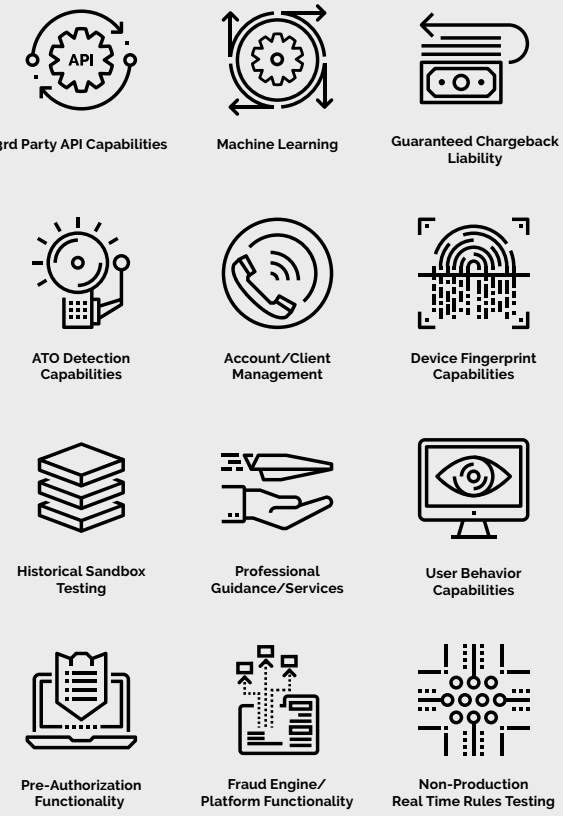
Handling 960 million transactions per year totaling over $150 billion, their volume is growing by 5-10% every month. They support clients' goals by focusing on fraud loss rates, fraud prevention program operating expenses, approval rates, account takeovers, suspicious AML activity count, and payment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

Solutions and functionality:

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

sardine

At a Glance:



Sardine

Specific capabilities include:

Device Intelligence and Behavioral Biometrics:

- **Sardine's** native app and Web SDK allow customers to gather and analyze not only end-user device data (Device Intelligence), but also how the user interacts with their device (Behavioral Biometrics). The combination provides out-of-the-box metrics that can be used for event risk scoring, age detection, remote access tool (RAT) identification, and bot detection.
- Various methods of fingerprinting are possible, including account and generic fingerprints.

Identity and Business verification:

- Customers can enable phone, email, address, and geo/IP location data enrichment to help validate user identities.
- Sardine offers eKYC/SSN verification, document verification (DocKYC) with selfie likeness, enhanced due diligence (EDD), and KYB services for advanced onboarding and identity verification.
- Includes out-of-the-box rulesets to support flexible KYC/KYB paths, step-up verifications, and weighted-sum scoring for workflows customized to risk profiles.

Rule Editor:

- **Sardine's** rule engine is prebuilt with over 4,000 features and a rule bank that includes detection templates for compliance and fraud risk scenarios.
- Users can conduct live testing in shadow mode or conduct back-testing of rule performance against historical transaction and user data.
- Multiple real-time rulesets can be created and run in parallel to protect against different risk vectors.
- Clients can choose between different execution methods for each rule set, combining the outcomes of triggered rules using different aggregation functions.
- It's also possible to write rules using a no-code rule editor or using an expression language.

Payment Fraud:

- The platform offers transaction risk insights and scoring utilizing machine-learned models trained for—and across—verticals with access to bank consortium data. The platform supports bank transactions (ACH), card transactions (both on the acquiring and issuing sides), and cryptocurrency transactions.
- Checkout fraud protection is also provided (including chargeback protection).

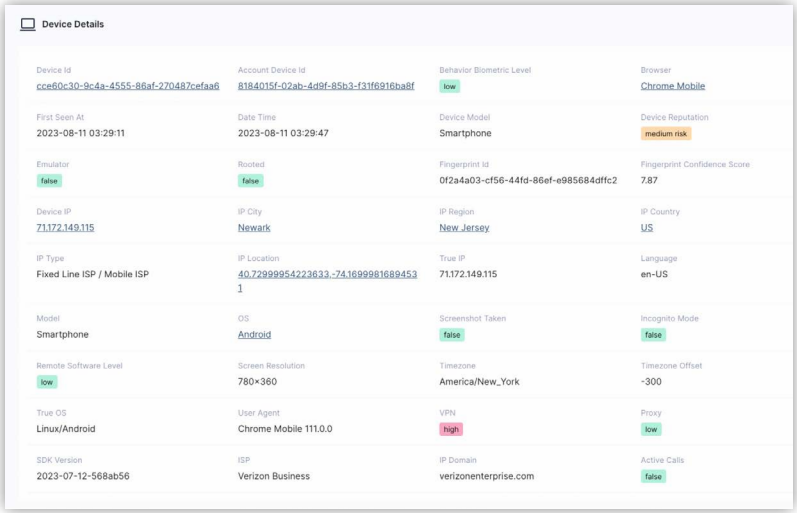
Compliance:

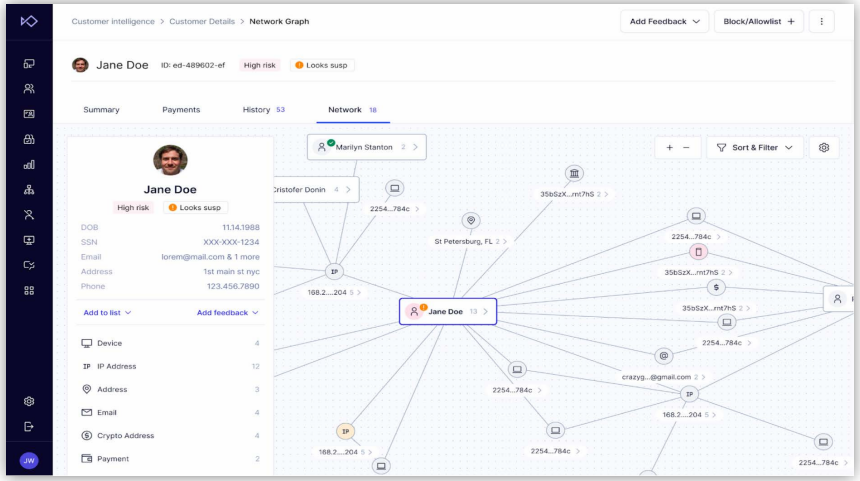
- **Sardine** offers a compliance solution that includes sanctions screening and monitoring services for individuals and businesses, crypto wallet screening, AML transaction monitoring services, and case management.

- They also offer a Sponsor OS product for fintech sponsor banks and Banking-as-a-Service (BaaS) companies, which helps them manage all the child program accounts via a dashboard interface. This includes support for a portfolio view of programs, grandparent-to-grandchild account hierarchy, and rule management for the portfolio of programs.

Reporting:

Sardine's standard dashboard includes an analytics area that provides filterable data visualizations and tables showing customers, transactions, non-transaction events, anomalies, and API usage. The data within the charts and tables can be exported for analysis in other applications via standard file types like .csv and Excel spreadsheets.





Services offered:

Sardine currently offers three levels of support:

- **Basic support: Sardine's** basic support tier includes email support with a one-business-day service level agreement and access to the platform's knowledge base. Standard contracts with basic-level support come with four weeks of premium-level support included immediately after integration.
- **Premium support:** This next-level support tier includes a dedicated Slack channel with **Sardine** Support Engineers, a dedicated Account Manager, and access to an auxiliary Sardine team (such as a risk analyst, ML engineer, and fraud ops). Premium support subscribers also receive bi-weekly calls and rule-creation assistance.

- **Enterprise support:** Sardine's enterprise-level tier includes premium support plus additional fraud program consultation, regular monitoring of rule performance and gaps, training, and expert guidance on optimizations according to the customer's specific use case.

Integration:

For back-end requests, **Sardine** provides the ability to integrate via API.

For front-end Device Intelligence and Behavior Biometrics, Sardine provides various SDKs to collect data:

- Examples of native app options include Native iOS and Android, Flutter, React Native, Xamarin, and VGS.
- Examples of web options include ReactJS, JS, and VGS.

For clients who onboard sub-customers of their own, **Sardine** coordinates the integration for each sub-client individually.

The timeline from signature to launch varies by customer and urgency. A typical example of effort and timeline:

- Design work requires approximately 0-2 weeks
- Front end and back-end engineers are required for approximately 2-3 weeks of actual active development work
- Deployment is scheduled as the final step in the process

Average response times depend on the use case, as some use cases may require enrichment to third-party data sources. However, a general average/v1 customer's API response time is less than one second. The device intelligence will send a response in 200-300ms. Sardine's responses are synchronous, so merchants can expect to receive a risk level via the API response. (Integration Guides can be found at https://docs.sardine.ai/)

Sardine offers customers pre-built rules that can be activated in shadow or live modes. The most effective rules are automatically accessible in customer dashboards. Customers can also access more rules from a constantly updated rule template library, which incorporates insights from the **Sardine** customer network. Finally, customers have the option to create custom rules using a no-code rule editor.

When it comes to rule management, customers have the ultimate responsibility for determining which rules are active in their production environments. In many cases, customers collaborate with **Sardine** Account Managers and Risk Analysts to strategize rule management. **Sardine's** Data Science team regularly provides customers with suggested additional rules to enhance performance.

Proof of Concept:

Since **Sardine** collects passive signals to detect fraud in real time, they strongly recommend that those who wish to engage in a POC

integrate their Device & Behavior SDKs and APIs. It's also a good idea to test the efficacy of the service using live traffic over a defined period. Back-testing is acceptable when limited to specific use cases that don't rely on real-time customer session data, such as AML transaction monitoring and payment fraud detection.

Pricing:

Sardine offers a combination of flat fee and transaction-based pricing. The flat fee grants customers access to a comprehensive fraud management dashboard, which allows for investigation, workflow management, and reporting. The transaction-based pricing applies to the insight and intelligence service they offer on a per-transaction basis.

12-month roadmap:

The **Sardine** team has much in the pipeline in the coming year, including:

Automated rule suggestions

- It will soon be easier and faster to create new rules or pull them from a rule library compiled across **Sardine's** network.

Custom data aggregations

- These will make it possible to flexibly employ unique strategies combining scoring model outputs to better suit your specific use case.

SAR filing

- Suspicious Activity Reports (SAR) creation and filing will soon be simplified.

Signifyd

Signifyd's Commerce Protection Platform helps address fraud challenges at key conversion points across the ecommerce shopper journey, from account creation to return request. By eliminating fraud and abuse throughout the funnel, the platform allows merchants to protect revenue, trust customers, and promote growth. **Signifyd** has been ranked No. 1 Payment Security and Fraud Prevention vendor in Digital Commerce 360's Retail Top 1000 for the last three years. **Signifyd** supports a large number of enterprise customers, including two of the world's top three online retailers. **Signifyd** is headquartered in San Jose, California, with locations in Denver, New York, Mexico City, São Paulo, Belfast, and London.

Signifyd helps merchants:

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

Signifyd

At a Glance:

eliminate the roadblock of fear to enable fearless growth. The platform allows merchants to more confidently launch new products, expand internationally, offer omnichannel shopping experiences, and establish flexible business policies and customer rewards.

Platform, Solutions & Functionality

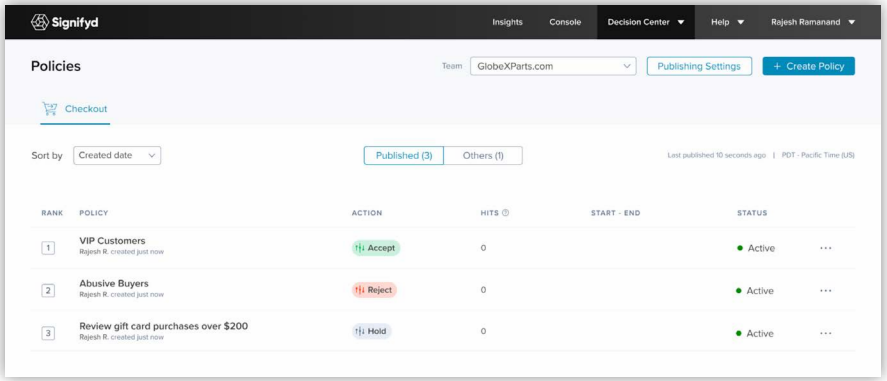
Signifyd's Commerce Protection Platform is designed to drive greater conversions while reducing risk.

Signifyd's Commerce Network: As the foundation of the Commerce Protection Platform, **Signifyd's** Commerce Network combines identity and intent intelligence from thousands of global ecommerce retailers with Payment Service Provider (PSP) data, issuer insights, and a merchant's own consumer data to proactively block emerging fraud and abuse trends. With a high rate of online purchases made by consumers previously seen across the Commerce Network, legitimate customers can be recognized and expedited through the digital shopping journey.

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

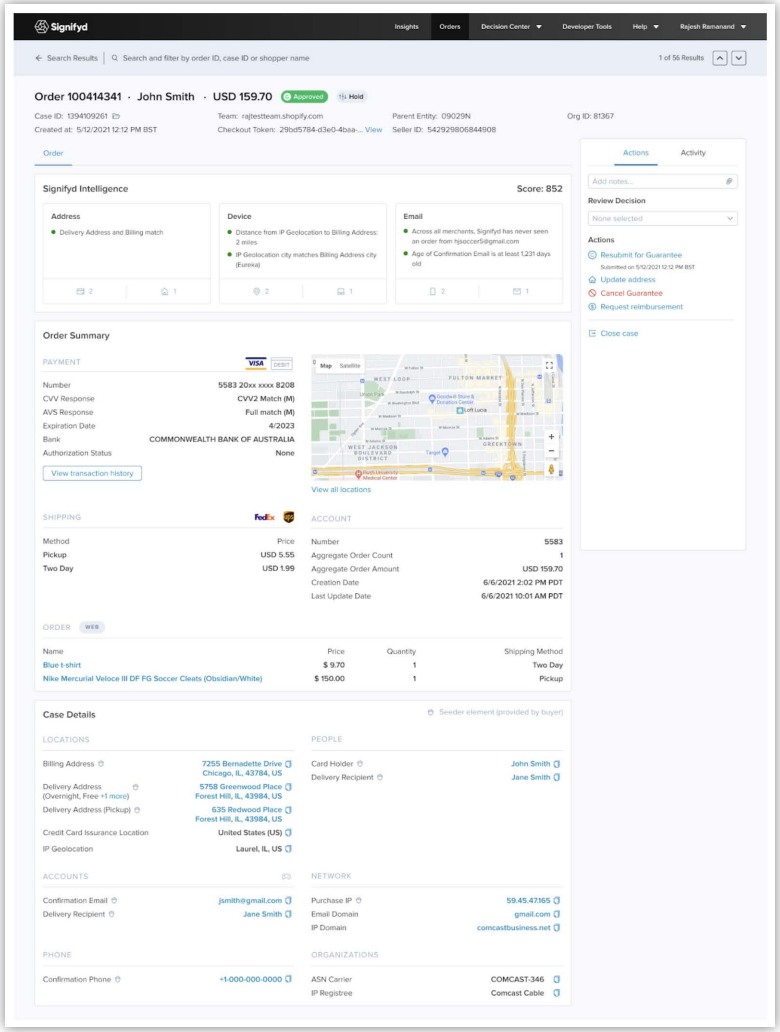
The platform features three core modules, which provide a window into **Signifyd's** network and engine:

- **Decision Center** to create and enforce custom business policies
- **Agent Console** to view transaction-level information and variables used to inform decision making
- **Insights Reporting** to provide the business intelligence and benchmarking necessary to optimize performance over time



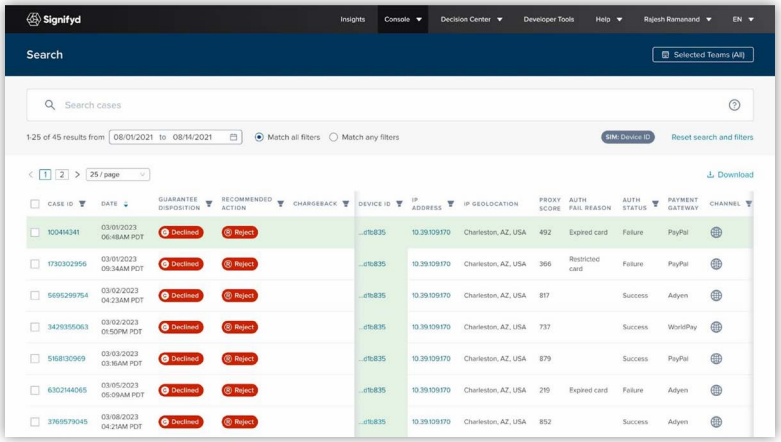
Similar to the need for transparency into decisions, merchants migrating to machine learning from rules-based platforms want to maintain control over their unique business policies and the customer experience they drive. **Decision Center** allows a risk

or fraud management team to draw on network insights as well as business-specific data when creating and enforcing policies specific to their business. Merchants can create, test, deploy, and manage all of these policies directly from **Decision Center**.

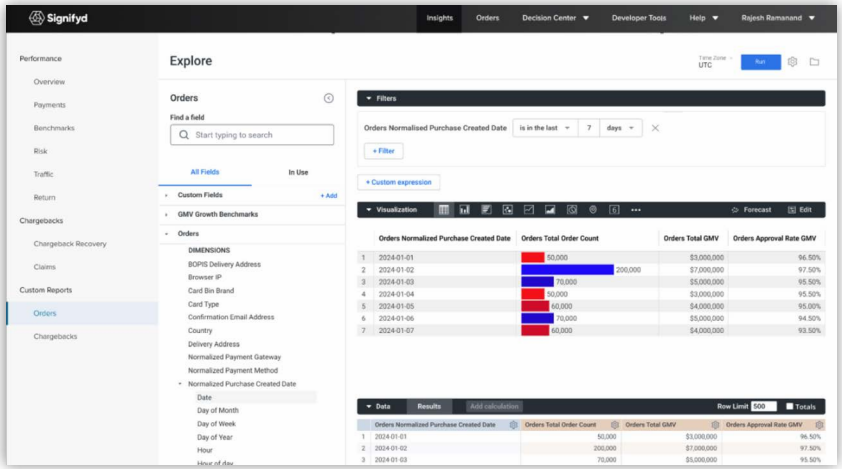


Agent Console is an interface that gives agents visibility into transaction-level data. Agents can drill into the data variables used to inform order decisions made by **Signifyd's** machine-learning model, as well as indicators into which variables weighed most heavily into decisions—both positive and negative. **Agent Console** also gives agents the ability to make modifications to an order (i.e. update delivery address) as well as to submit claims for any orders that have been covered by **Signifyd's** chargeback liability.

A feature of **Agent Console** is **Power Search** – an advanced searching capability that allows users to investigate order connections and surface patterns of fraud and abuse. With this information, merchants can quickly leverage insights to deploy more effective business policies.



As merchants make the shift from legacy rules-based solutions to machine-learning platforms, the transparency provided by **Agent Console** helps build merchant trust in **Signifyd's** decisioning model and allows merchants to discover patterns that may indicate emerging fraud trends.



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

In addition to the three modules, **Signifyd** also provides six products that use network intelligence to address common business challenges:

- **Account Integrity** analyzes behavioral and device data to protect customer accounts from malicious schemes. By assessing risk across account creation, login, modification and check out, **Signifyd** can accurately distinguish between fraudsters and the true account holder – applying friction only when necessary to mitigate risk.
- **Authorization Rate Optimization** bridges the merchant-issuer data gap via direct connection to issuing banks. This allows orders sent for authorization to be enriched with identity and intent intelligence from the **Signifyd** Commerce Network, proving an order is legitimate. Removing fraudulent orders pre-auth can help increase authorization rates over time, as only the cleanest traffic is sent to the banks. This allows banks to authorize orders that otherwise would be falsely declined.
- **Guaranteed Fraud Protection** pairs order automation with a financial guarantee against fraud chargebacks on all approved orders. This shifts liability away from the merchant, allowing them to optimize for revenue attainment and pay $0 in fraud losses on approved orders.
- **Complete Chargeback Protection** evaluates orders at checkout and delivers decisions backed by a financial

guarantee against both fraud and non-fraud chargebacks (ie INR, SNAD, processing errors etc.) on all approved orders. The result is elimination of all chargeback losses for merchants.

- **Chargeback Recovery** combines intent intelligence from the **Signifyd** Commerce Network with merchant-specific chargeback data to identify abusive shoppers and dispute suspicious claims automatically. The functionality also helps fine-tune **Signifyd's** machine-learning models over time by learning which decisions result in chargebacks.
- **Return Abuse Prevention** evaluates incoming return requests to deliver recommendations on how and whether to proceed with a refund. The product allows merchants to incorporate **Signifyd's** long history of consumer behavior with their specific return policies to block abusive returns, streamline customer interactions, and automate refunds for good shoppers.

Technical Integration

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

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

Professional Services

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

In development over the next 12 months:

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

- New issuer partners to the **Signifyd** Commerce Network to improve auth decisioning accuracy
- New integrations with leading return platforms to embed **Signifyd's** return abuse policies
- Greater configurability of consumer-facing decision workflows
- Enhancements to our account integrity solution, providing more holistic protection across the account journey

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.

ClearSale

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

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

False Declines Cost More Than Fraud

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

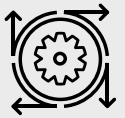
While most ecommerce merchants focus on managing fraud and chargeback costs, the cost of revenue lost to false declines (also known as false positives) is far more expensive.

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

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

ClearSale

At a Glance:



Machine Learning

Fraud Engine/ Platform Functionality

User Behavior Capabilities

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

DataVisor

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

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

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

DATAVISOR

At a Glance:

3rd Party API Capabilities

Device 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.

Feedzai

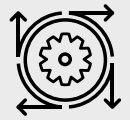
Feedzai attempts to provide a machine-learning-based fraud platform to help risk professionals do the work of data scientists using a guided, self-contained environment. Through **Feedzai DS**, teams are provided with a way to create advanced machine-learning fraud models. With extraction of features,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

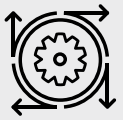
Feedzai chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

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

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

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

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

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

NOFRAUD

At a Glance:

Fraud Engine/ Platform Functionality

Guaranteed Chargeback Liability

Machine Learning

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

NOTO

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

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

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

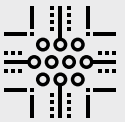
Solutions and Functionality

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

NOTO

YOUR DATA. YOUR WAY. NO LIMITS.

At a Glance:



Non-Production
Real Time Rules Testing

Fraud Engine/
Platform Functionality

Professional
Guidance/Services

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

Outseer

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

Products, Solutions and Technologies:

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

OUTSEER
An RSA Company

At a Glance:

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

Ravelin

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

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

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

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

Ravelin

At a Glance:

Fraud Engine/ Platform Functionality

Operational Support

Pre-Authorization 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.

Sift

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

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

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

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

At a Glance:

3rd Party API Capabilities

Machine Learning

Fraud Engine/ Platform Functionality

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

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.

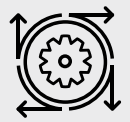
When information is added, their models will adapt and evolve to those patterns. They say the models adapt and detect patterns of fraud before they are perceptible to human analysis. Also, manual rules are arranged into code and fed into their machine-learning models.

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.

Vesta

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

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

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

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

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

Solutions and functionality:

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

At a Glance:

Guaranteed Chargeback Liability

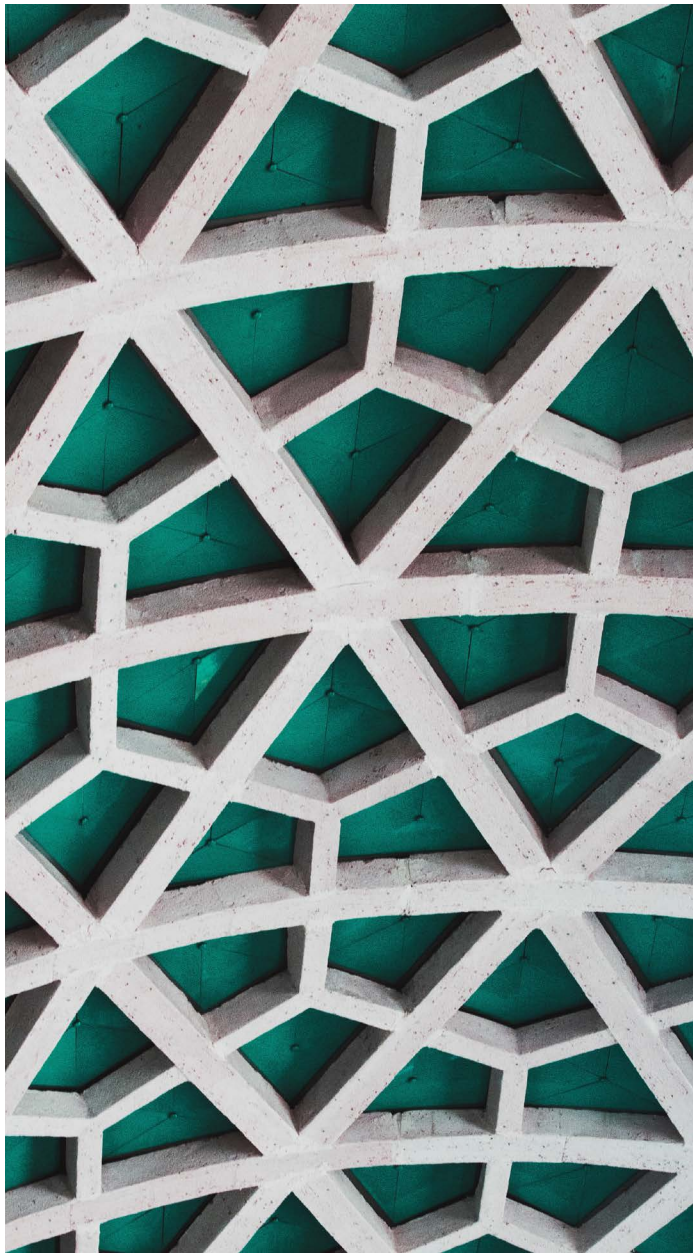
Machine Learning

Fraud Engine/ Platform Functionality

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

Identification & Data Verification

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



TransUnion

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

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

TruValidate solutions help create friction-right experiences, allowing 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, false positive rates, manual review rates, customer lifetime value, abandonment rate, operational efficiency (IVR/contact center), fraud capture rate, average call handle time, lifetime customer retention, customer satisfaction, and conversion rate.

At a Glance:

3rd Party API Capabilities

Machine Learning

Guaranteed Chargeback Liability

Account/Client Management

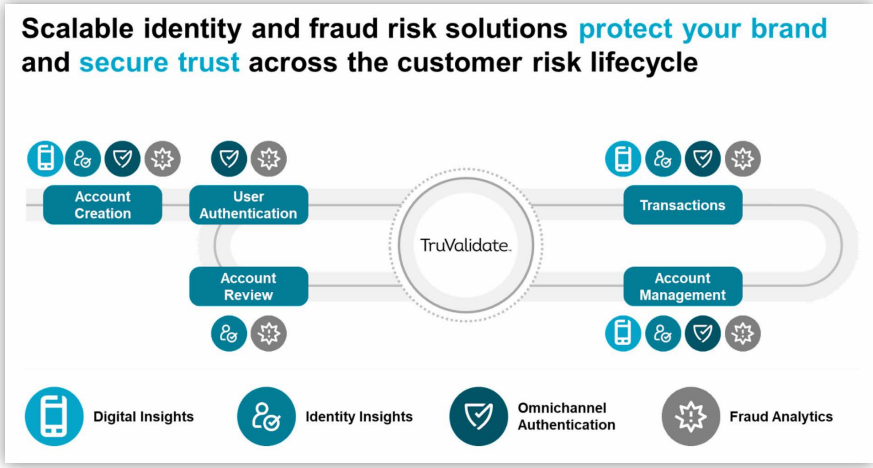
User Behavior Capabilities

Pre-Authorization Functionality

Fraud Engine/ Platform Functionality

Solutions and functionality

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



Identity insights

Provide great experiences and expose fraud risks by confidently verifying consumer identities against robust credit, non-credit, and digital data sources from around the world.

- **Identity Verification:** Verify and resolve consumer identities with high match rates and significantly reduced friction.
- **Fraud Alerts:** Gain key insights into suspicious behavior in real time through analytics-based, high-performing fraud alerts that can be configured to brand priorities and use cases.
- **Document Verification:** Reduce customer abandonment and increase customer acquisition by verifying consumer-provided documentation, including device reputation checks and verification of PII against credit header data.
- **Device-based Authentication:** Speed up logins for known customers by removing extra friction for recognized devices
- **Email & Phone Verification:** Expedite customer onboarding while recognizing fraud risk via detection of risky emails and phone numbers.

Digital insights

Improve customer satisfaction while determining the riskiness of anonymous users in real time through insights into device recognition, context, and behaviors.

- **Device Proofing:** Maximizes digital fraud capture earlier in the consumer journey and minimize friction against good customers through complementary signals of device reputation, device-to-identity linkages, and behavioral analytics.

- **IP Intelligence:** Confirms the legitimacy and origin of web traffic for geo-compliance and fraud mitigation.

Omnichannel authentication

Provide smooth, secure, seamless experiences across call center and digital channels. Leverage phone and device data to separate legitimate consumer interactions from potentially risky ones to authenticate established users and mitigate account takeover fraud.

- **Step-up Authentication:** Leverage data from phone carriers to alert for SIM swap, call forward, and phone reassignment events to ensure the safe and friction-right delivery of one-time passcodes.
- **Inbound Authentication:** Pre-answer caller identification, risk assessment, and authentication solution to reduce average call handle time, improve caller experiences, and prevent fraudsters from reaching the IVR or agent.

Fraud analytics

Streamline transactions, detect hidden connections, and proactively monitor threats with valuable risk insights through superior data, analytic expertise and customized, purpose-built models.

- **Models and Scores:** Stay ahead of evolving fraud threats with custom-built fraud prevention models and analytics.
- **Model Attributes:** Ingest raw model attributes to adapt to evolving fraud circumstances proactively. Meet specific and emerging fraud challenges while building trust with your customers.

Socure

Socure is a market leader in the identity verification and fraud prevention industry. Its predictive analytics platform applies AI and machine learning (ML) techniques with thousands of sources of trusted online/offline data and behavioral signals to verify every element of identity in real time, including government documents, email, phone, address, IP, device, date of birth, and SSN.

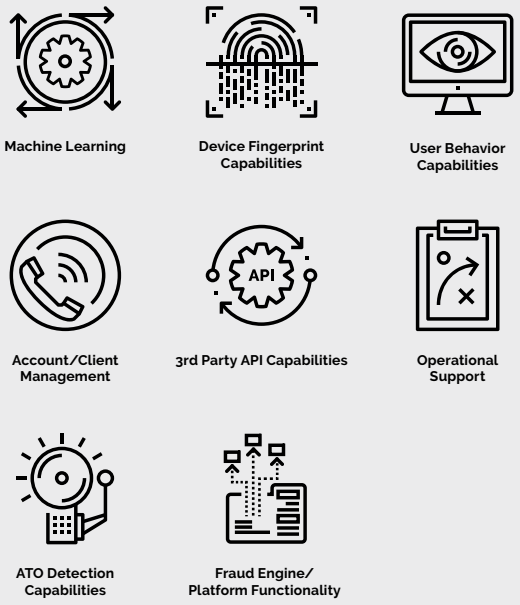
Socure's patented AI and ML platform powers an elevated standard for seamless Know Your Customer (KYC) and compliance, fraud detection, ID document verification, and bank account ownership validation using a purpose-built, end-to-end solutions suite (Socure ID+) via a single API. Bolstered by over 150 million rows of outcomes in the past year, Socure's database totals two billion known good and bad identities. This results in robust, industry-leading accuracy to unlock identity trust for digital interactions and engagement at onboarding and throughout the customer journey for top companies across all verticals and geographies.

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

Socure supports over 2,000 customers and enables trusted customer transactions across the financial services, marketplace, government, gaming, workforce, healthcare, telecom, and ecommerce industries. Customers include nine of the top 10 banks, 13 of the top 15 card issuers, the top three MSBs, the top payroll provider, the top credit bureau, the top online gaming operator, top buy-now-pay-later (BNPL) providers, and over 400 of the largest fintechs. **Socure** helps these clients better assess first-party, third-party and synthetic ID fraud risk, increase auto-acceptance, and reduce false positives and friction.

SOCURE

At a Glance:



And they do it while optimizing the digital customer experience at application, account update, password reset, high-value transactions, and across the customer lifecycle.

Solution Highlights

Socure Risk Insights Network

The **Socure** Risk Insights Network (the Network) is at the center of the **Socure** ID+ fraud and identity verification solution suite. It is not a standalone product, but rather the strategic, foundational bedrock that powers **Socure's** accuracy and solution innovation. The Network provides companies of all sizes and across all industries with valuable, trustworthy risk intelligence to onboard more legitimate identities and prevent fraud.

- First, the Network ingests proprietary insights from **Socure** ID+ API production transactions, client feedback data on risk outcomes, and third-party identity data from authoritative sources.
- Next, **Socure's** advanced analytics tracks identity behavioral patterns, such as how often an identity emerges in the financial ecosystem and which new or previously correlated PII elements appear alongside the identity, to evaluate risk.
- Finally, the resulting insights around trustworthy entities and risky identity attributes are circulated back into the **Socure** ID+ solution suite to enrich the accuracy of the products, thereby promoting the absorption of increasingly more refined feedback data into the Network.

Socure Sigma Fraud Suite

Sigma Identity Fraud V4 is a fully integrated, internally developed, identity fraud solution suite that fuses personal identifiable information (PII) validated by thousands of data sources, a real-time network, and anomaly detection. Digital and behavioral risk signals offer an instant—and near 100% accurate—identity fraud decision in less than 150 milliseconds, with five nines of uptime availability.

It includes two central innovations: Entity Profiler and Integrated Anomaly Detection.

- **Entity Profiler** is a highly sophisticated ML solution that fuses digital footprints and session intelligence with authoritative data in a singular view of identity. By considering the recency,

frequency, and context of historic transactions and behavior, this approach allows for a more dynamic and accurate assessment of identity and device ownership while adapting to new privacy standards. **Socure's** system can confidently assert the identity of a consumer who has consistently utilized similar PII, IP geo-location, mobile devices, operating systems, and browser languages over a span of multiple years and across varying institutions. This information allows them to create a unique and persistent device ID.

- **Integrated Anomaly Detection** provides highly effective mitigation against some of the most advanced Generative AI threats. This powerful solution is engineered to analyze identity behaviors across various levels—company, industry, and financial networks— identifying thousands of risk factors in real-time that legacy approaches miss. It excels in detecting unusual real-time user behavior patterns, offering protection against sophisticated, high-volume fraud attacks. With this technology, customers are equipped to swiftly identify and respond to threats, such as a sudden increase in applications from device farms, tumbled emails, muling activity or unknown VoIP providers.

Socure's Sigma Identity Fraud V4 solution captures up to 99% of all ID fraud in the top 5% of riskiest users compared to the industry average of just 37% from credit bureaus and other fraud providers. Meanwhile, it provides a greater than 40% absolute reduction in false positives, relative to **Socure's** prior, best-in-class Sigma ID version, allowing customers to accept more good consumers–all in under 150 milliseconds.

By maintaining radical accuracy, **Socure** customers can consistently expect a 20x return on investment. The largest value drivers include increased revenue through false positive reduction, ID fraud losses being reduced to near zero, and total cost of ownership reduction. Unnecessary point solution providers are turned off and manual review is reduced from the industry average of 10-15% to less than 5%.

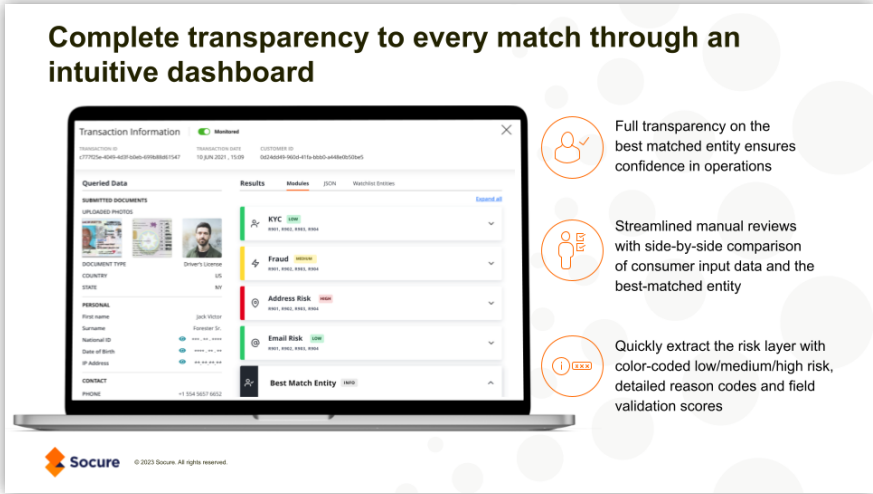
Socure's Email, Phone, and Address RiskScores

Socure's email, phone and address RiskScores, as well as ownership correlation, can be applied in a number of situations. In one key use case, organizations leverage the solutions to prevent account takeovers by assessing phone, address, name and email changes in account profiles–often the first steps in an ATO attack. They're also used for progressive onboarding if limited identity attributes are collected by a given consumer-facing service over time.

Socure's RiskScore products deflect fraud from faked, stolen, and invalid email accounts, phone numbers, and physical addresses without adding friction to any part of the customer experience at onboarding, account change or transaction. **Socure** has advanced features that can identify email pattern-based fraud attacks like

gibberish emails, alias emails, email tumbling, invalid domains, and more. Through POC's, **Socure** has proven to give a 12% lift in coverage with 15% more fraud capture than every single competitive email solution, verify 28% more phone numbers with 40% greater fraud capture than the leading phone finder providers, and can verify 20% more addresses than anyone else in the market.

Socure's identity element-specific machine learning models are trained with 50+ element-specific variables to predict the likelihood of fraud and risk through the evaluation of attributes related to geolocation, age, velocity, linkages, out-of-pattern behavior, IP address, and more. Socure's service has greater than 96% coverage for emails, phones, and addresses.



Digital Intelligence Suite

Socure's Digital Intelligence Suite consists of three sophisticated services working together to provide a real-time view of online events. Digital Intelligence brings together Device Intelligence, Behavioral Analytics, and an Entity Profiling service to go beyond antiquated device fingerprinting techniques that no longer work on modern, privacy-conscientious mobile devices and browsers. Instead of relying on fixed identifiers,

Socure employs a privacy-forward approach to associate device, behavior, network, and location patterns at consortium and network scale—evaluating what is typical for an individual across elements like email, IP, and location history. Analyzing over 500 correlated feature candidates through machine learning experiments, **Socure** ties together data dimensions through adaptive behavioral profiles rather than binary match points. **Socure** drives risk insights from a fusion of corroboration across attributes, plus holistic evaluation of activities over reliance on discrete IDs. This, integrated into the company's Sigma Identity V4 model, lets Socure crystallize differentiators between regular variation and potential risk fluctuation with unparalleled precision–all in real-time.

Sigma Synthetic Fraud is a purpose-built synthetic identity fraud detection solution that delivers holistic protection through multi-layered controls to block harmful synthetic identities from entering an ecosystem at account creation. The model employs advanced

machine learning techniques cyclically trained with expert human-supported analysis to mitigate rapidly evolving and complex synthetic patterns. Sigma Synthetic captures 71% of fraud in the top 3% of riskiest customers.

The solution can adapt to customers' decisioning strategy accordingly, whether the goal is to capture more synthetic fraud or create a lower-friction user experience. **Socure** can also help identify synthetic identities that have been accepted and exist within an organization's existing customer portfolio by conducting "scrubs" using synthetic fraud models.

Sigma First-Party Fraud is the industry's first holistic first-party fraud (FPF) solution that identifies repeat first-party fraud abusers across the financial ecosystem. Sigma First-Party Fraud predicts the likelihood of bad-faith disputes or payment defaults driven by confirmed, fraudulent activities for financial institutions and merchants. For instance, one initial result of **Socure's** proprietary consortium data study showed that consumers who were members of at least four consortium study participants were seen doing FPF by at least one member, 30% of the time.

Identification of first-party fraud risk up front will result in a reduction of account charge-offs and follow-on chargeback losses and dispute resolution costs for institutions and ultimately establish a holistic financial ecosystem of trust.

Socure Compliance Suite

Socure's Compliance Suite represents one of the most sophisticated platforms for compliance professionals with a complete, purpose-built solution to solve today's toughest compliance challenges while delivering the highest level of compliance possible. **Socure** offers compliance professionals market-leading data coverage, precision and accuracy, and world-class tools to efficiently manage operations.

Socure Verify provides non-documentary CIP (Customer Identification Program) verification with very high levels of precision and accuracy, reasoning, address verification, matching, and graphing for clear identification of risk and alignment with policy. **Socure's** triangulated data approach leverages AI & ML to verify an identity across multiple trusted sources and then correlates thousands of identity data points—online and offline—to resolve to a single best-matched entity providing industry-leading results:

- **Accuracy:** While legacy vendors misclassify more than 5% of transactions and are unable to verify certain segments 10% of the time, **Socure** accurately verifies up to 99% of mainstream populations and up to 94% for hard-to-identify populations such as Gen Z, millennial, credit-invisible, thin-file, and new-to-country, ensuring inclusive access for all.
- Highly Accurate Gen Z data coverage: According to historical

POCs, **Socure** can verify 70% of 18 year-olds when opening their first financial accounts—30% more than legacy providers—and up to 94% of 18 to 25 year-olds. They also deliver industry-leading verification rates for 13 to 17 year olds.

Socure's proprietary models outperform long-held industry standard techniques and perform precise matching, even in the presence of variations, misspellings, or different name orders.

Socure's Global Watchlist Screening with Monitoring ensures regulatory compliance and reduces risk by verifying the integrity of a customer base during onboarding and ongoing in real-time to immediately alert you to customer status changes. **Socure's** sophisticated matching algorithms, proprietary data, and continuous monitoring deliver accurate and uninterrupted compliance with KYC/CIP and sanctions enforcement requirements.

Integrated case management offers side-by-side comparison of customer data and watchlist matches to quickly identify risk, expedite reviews, and provide full auditability of decisions. Global Watchlist Screening with Monitoring provides three tiers of service, with customizable coverage for OFAC, SDN, FinCEN, global sanctions and enforcement lists, PEPs, adverse media, and more.

Socure's Decision Module offers simple no-code, real-time management of customer onboarding decision logic. This includes identity, watchlist, and fraud risk parameters that guide whether to accept, decline or flag a consumer for further review. It also provides streamlined reporting and audit capabilities. Additionally, it offers the industry's first simulation engine to model the impacts of potential logic changes using historical customer transaction data for greater assurance of desired outcomes.

Socure's Control Center offers sponsor banks a comprehensive management dashboard, providing real-time visibility into key compliance Key Performance Indicators (KPIs) while ensuring compliance with sponsor bank policies across their entire portfolio of bank partners. Sponsor banks can monitor bank partner fraud rates and Customer Identification Program (CIP) approvals. They can also assist with timely resolution of watchlist screening cases, and more. The platform enables sponsors to quickly update policies, test the impact using historical customer data before implementation, and add new monitoring rules.

Document Verification

Socure's Predictive DocV (DocV) verifies a consumer's government-issued identity document against their facial biometrics with machine-learning-driven decisioning to identify more good customers and keep out the fraud. After agreeing to the consent form, the consumer begins a fully automated flow. Guided image capture enables an easy scan of the front and back of the ID extracting human- and machine-

readable components. After scanning the document, the consumer takes a quick selfie, which is biometrically matched to the photo on the ID with NIST PAD L2 liveness detection to stop spoofing attacks. Real-time image quality checks after each capture enables industry-leading consumer conversions with accurate, automated decisions in under two seconds.

The benefits of DocV extend from fraud prevention to consumer conversion and implementation ease. With customizable logic to adjust based on a customer's own risk posture, DocV fits a wide variety of use cases whether it's as a step-up solution for the riskiest consumer segments, as a fallback for identity verification, or as a top-of-funnel solution such as what is required for gaming and crypto industries. The solution's lightweight SDK integration (both native and web based) as well as the no-code customizable branding and workflows, offer expedited implementation timelines. With patented fake ID detection, innovative fraud models, and predictive risk signals built on the most comprehensive identity graph, DocV leads the identity verification market with radical accuracy, unmatched speed, and a superior user experience.

Account Validation

Socure Account Intelligence

Socure Account Intelligence instantly verifies domestic bank account status and ownership, prior to ACH payment transactions or funds disbursement. Only the consumer or business name as well as the bank account and routing numbers are needed for this real-time service, which establishes trust between accounts and supports regulatory compliance.

The product is suited for any client or industry in which an ACH payment is being made (e.g., bank account funding, disbursement of government benefits, bill payments, insurance payouts, merchant payments, and peer-to-peer payments). Because of **Socure** Account Intelligence's core benefits of establishing bank account trust and determining payment return risk, users can expedite disbursements of funds, guard against payment fraud, and adhere to ACH requirements, all while supporting reduced customer friction.

Socure is capable of processing hundreds of transactions a second and billions of transactions a year. Beyond its scale, it prides itself on customer service, which is treated as more than problem resolution. They regularly collaborate on best practices, trends, and new use cases to give their customers better insights. **Socure's** subject matter experts remain at the ready to weigh in on anything from product to data science to legal.

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.

ARKOWL

At a Glance:

3rd Party API Capabilities | Professional Guidance/Services | Pre-Authorization Functionality

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

Ekata by Mastercard

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

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

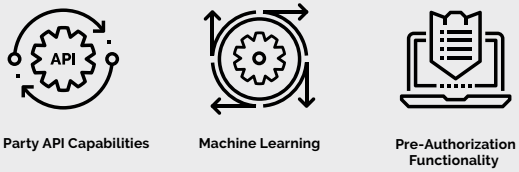
Identity Network analyzes patterns of how consumers information is being used in digital interactions with behavioral patterns and transaction-level intelligence.

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

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

ekata by

At a Glance:



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

Emailage

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

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

emailage™
GLOBAL FRAUD PREVENTION

At a Glance:

3rd Party API Capabilities

Account/Client Management

Machine Learning

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

Flashpoint

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

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

FLASHPOINT

At a Glance:

ATO Detection Capabilities

Pre-Authorization Functionality

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

GB Group

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

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

GBG

At a Glance:

3rd Party API Capabilities

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

GeoComply

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

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

Four typical use cases for **GeoComply**:

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

GEOCOMPLY

Empowering The Future Of Digital Trust

At a Glance:

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

Intent IQ

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

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

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

At a Glance:

3rd Party API Capabilities

ATO Detection Capabilities

Pre-Authorization Functionality

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

LexisNexis Risk Solutions

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

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

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

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

LexisNexis® RISK SOLUTIONS

At a Glance:

3rd Party API Capabilities

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

Nuance

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

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

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

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

NUANCE®

At a Glance:

3rd Party API Capabilities

Machine Learning

Account/Client Management

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

Oneytrust

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

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

oneytrust

At a Glance:

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

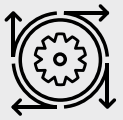
Onfido

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

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

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

At a Glance:



Machine Learning

ATO Detection Capabilities

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

Pipl

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

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

At a Glance:

3rd Party API Capabilities

Professional Guidance/Services

Pre-Authorization Functionality

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

TeleSign

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

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

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

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

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

TeleSign

At a Glance:

ATO Detection Capabilities

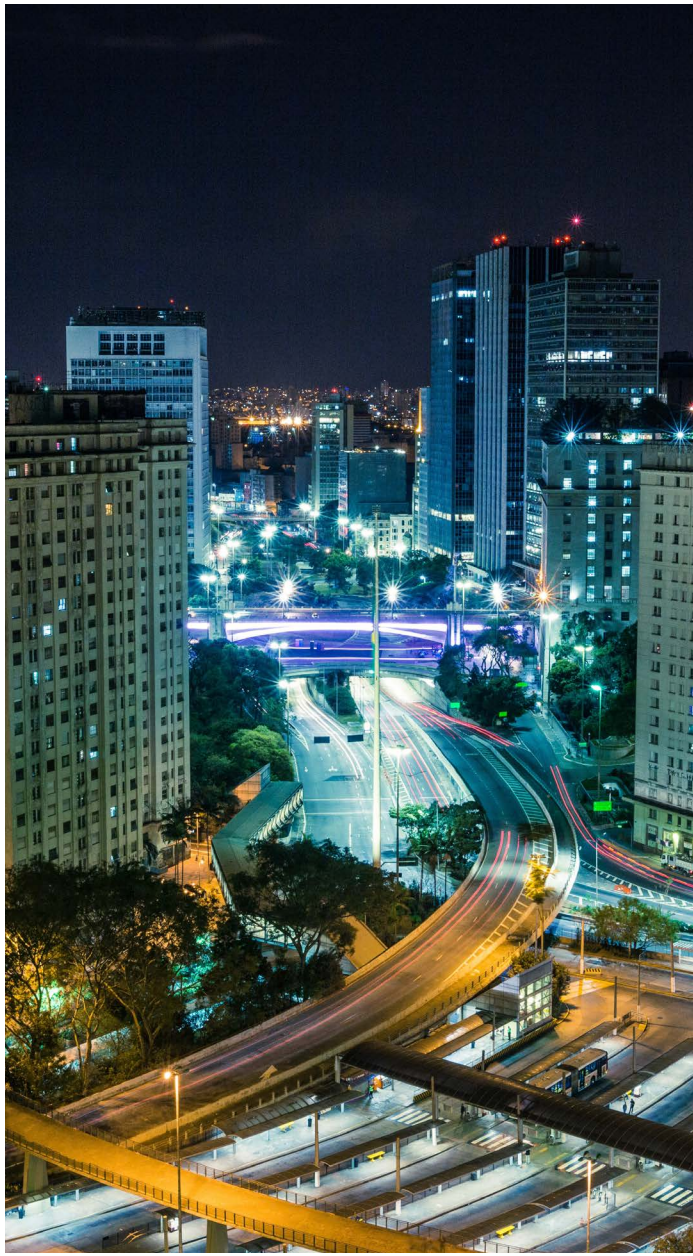
Account/Client Management

Pre-Authorization Functionality

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

Chargeback Management & Platforms

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



Accertify Chargeback Services

Accertify provides fraud prevention, chargeback management, Account Protection, refund and returns, Strong Customer Authentication (PSD2), 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 make it possible for clients to address risk pain-points across the entire customer journey—from account creation to authentication, activity monitoring, payment, and disputes.

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

Accertify Chargeback Services

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

At a Glance:

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

Accertify Chargeback Services

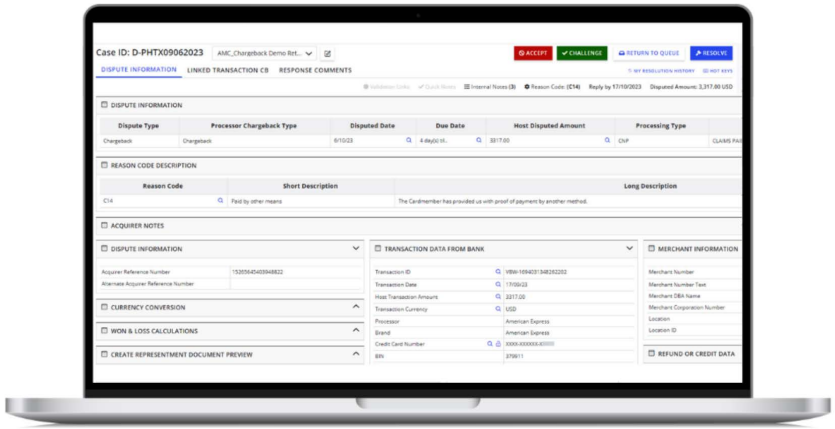


figure 1: user interface

Accertify's Chargeback Management solution can reduce or even remove the manual resources required to manage and respond to chargebacks by incorporating full or partial automation into the process. It offers a software-as-a-service platform that clients can manage themselves or they can outsource the end-to-end management of chargebacks using **Accertify's** Strategic Risk Services offering.

The platform offers:

Automated Processor Integration: Accertify is integrated directly with most processors. Therefore, most chargeback files can be automatically and systematically imported (without human intervention) into the platform. In addition, chargeback responses can be automatically exported to integrated processors using similar technology.

Workflow Management: The platform has out-of-the-box workflows which focus on due dates and high dollars. It can create client-specific workflows based upon dollar values, chargeback reason, due date, client business needs, and other similar data points. It can be configured to highlight the most important chargebacks to be worked based on industry and client requirements. Examples of this would be chargebacks on future flights, high dollar chargebacks, VIP loyalty customer disputes, most likely to win, etc.

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

Workflow

Accertify's automated document capture process eliminates manual processes traditionally required for uploading screenshots and printed documentation. In addition, when the workflow is coupled with data from the Fraud Platform or enhanced with compelling evidence from the client, the workflow can be designed

to create fully automated responses to the processors. This no-touch model works especially well for high-volume, less complex chargebacks.

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

Web-based Dashboards and Reporting

Insights provided in the reporting package allow clients to look at the big picture when assessing chargeback team operations and success criteria. The initial landing page has dashboards which display trends for recently worked items and a 12-week or 12-month won/loss trend analysis. It also provides a dashboard of which chargebacks are nearing their reply-by dates as well as what has been worked over the last few weeks. This provides a clear understanding if the merchant's staff are keeping up with inventory and the overall success which is being achieved.

For reporting purposes, users can select desired filters (load/resolution/sale date, agent identifier, reason code group, etc.) and can evaluate various aspects of the chargeback inventory as well as the chargeback team's productivity and success. Analyst performance is reflected in won/loss success ratios in total dollar, case count, and percentage amounts for cases manually reviewed and completed versus total cases accepted.

The platform not only provides insight into who last interacted with a chargeback but can also show an agent's average work duration for a specified period. Won/loss ratios can also be aggregated and grouped out by a reason code group, brand, and processor for trend analysis.

Lastly, the platform provides a way to export all data securely. Clients can define the data to be extracted and then run the extract immediately or schedule it for later use. This is extremely useful, as it allows merchants to utilize their own internal business intelligence tools.

Solution Integration

Accertify's Chargeback Management solution is directly integrated with the Fraud Platform, and information is automatically populated into the Chargeback Management solution and vice versa. The Fraud and Chargeback modules form a symbiotic relationship and seamlessly leverage and benefit from one another by staying synchronized and realizing their maximum potential through direct data share. If you are not a fraud client, **Accertify** supports direct integrations to merchant CRMs, which allows the platform to provide

the same level of automation and data as their joint solution provides.

Accertify also partners with Ethoca, Verifi, and American Express to enable pre-chargeback capabilities related to dispute deflection, transaction clearness, and chargeback alerts. This allows clients to react to change faster, including potentially avoiding the chargeback by stopping shipments, issuing refunds, improving fraud prevention rules and strategies, and enhancing model performance. They do all this while providing a best-in-class customer experience for their customers.

In 2024, **Accertify's** Roadmap will focus on a few key initiatives, including:

- Continuing to expand acquirer/processor global footprint
- Expanding and enhancing reporting capabilities and dashboard
- Developing a full end-to-end product for airlines and OTAs dispute collaboration
- Continuing to enhance the user interface with a focus on improving client experience
- Expanding full representment automation capabilities and modeling
- Expand current direct integrations to the major schemes

ChargeBacks911

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

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

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

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

At a Glance:

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

ChargebackOps

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

ChargebackOps offers two primary services:

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

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

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

Ethoca

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

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

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

ethoca™

At a Glance:

3rd Party API Capabilities

Account/Client Management

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

Sift Dispute Management

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

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

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

sift

At a Glance:

Operational Support

Account/Client Management

Professional Guidance/Services

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

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.