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

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

Sincerely,

The MRC

Table of Contents

The 2023 Paladin Vendor Report

The fraud landscape is increasingly complex. This report cuts to the chase. Every day at Paladin Group, we're in the thick of the fast-paced world of fraud solutions.Commerce and business models are ever-evolving. So it's crucial to remain focused on streamlining and maximizing the capabilities of organizational fraud management operations.

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

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

Because of the constant evolution of many popular fraud mitigation solutions, we decided to provide the Paladin Vendor Report (PVR) on an annual basis. And now, we're pleased to publish the latest: the 2023 Paladin Vendor Report. We've offered previous participants the chance to update their sections and incorporated additional participating vendors.

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

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

Introduction

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

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

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

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

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

Introduction

Core functionality icon key

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

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

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

Machine Learning – Matching algorithms to detect anomalies in the behavior of transactions or users.

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

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

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

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

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

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

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

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

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

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

User Behavior & Behavioral Biometrics

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

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.

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

NuData solutions are trusted by some of the world's largest brands to prevent fraud while offering a seamless customer experience.

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.

NuData Security
mastercard

At a Glance:

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

NuData

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 solutions cover the following use cases:

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

This can help clients by:

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

Reduced good user friction:

To eliminate unnecessary friction from your customer's online interactions, recognize returning users with behavioral insights that are based on their inherent behavior profiles. By leveraging insights from **NuData's** trust consortium and device intelligence, NuDetect can determine if a user is genuine, a human imposter, or bot.

This can help clients:

- Reduce false declines
- Remove unnecessary friction
- Offer a personalized user experience

NuData

Account creation risk: The sheer amount of consumer data available to malicious users presents a nearly limitless resource for launching new account fraud. When fraudulent new accounts use legitimate identity data, verifying these accounts can be difficult. Through a multi-layered approach, NuDetect evaluates whether a user is behaving like a legitimate user, a fraudulent human user, or a bot. The platform flags high-risk accounts so businesses can quickly intervene.

This can help clients:

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

Checkout fraud protection: Card cycling and testing, a practice that determines which stolen credit cards are active and available for use in a subsequent fraudulent purchase, has grown in popularity. NuDetect helps companies mitigate this automated behavior at checkout before attackers can take advantage of any information on their stolen cards.

This helps clients:

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

PSD2/SCA compliance: The recent enforcement of PSD2 regulation in Europe introduced Strong Customer Authentication (SCA) to reduce fraud and secure payments. In simple terms, SCA requires organizations to perform additional authentication steps throughout the user journey.

Many organizations turned towards SMS OTP challenges to achieve the possession factor of SCA. Building on top of that, NuDetect leverages behavioral biometrics and hundreds of data points from each OTP completion to recognize trusted users based on their physical behavior, thus achieving the inherence factor. This combination of possession and inherence eliminates the need for additional friction in the user journey, such as a Knowledge Based Authentication or active biometric (face ID, touch ID, etc.).

The technology supporting NuData solutions:

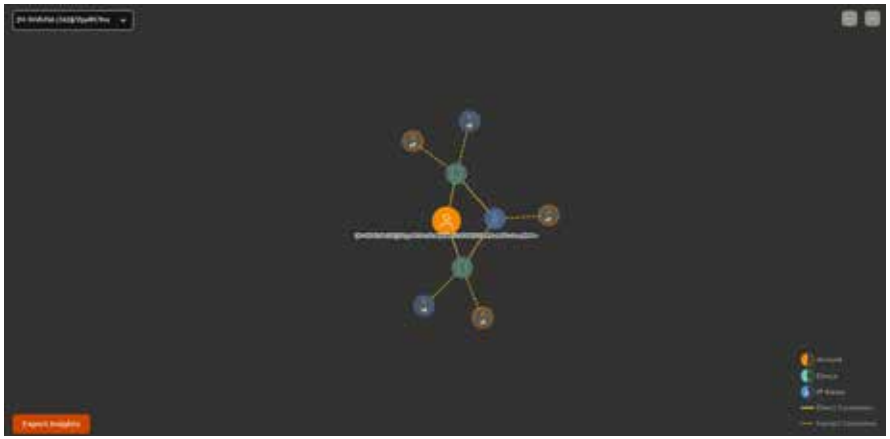
NuData uses a multi-layered approach to verify users online through traditional and behavioral methods. These layers identify anomalies, spoofing, or unexpected user behaviors and share the gathered intelligence with clients in real time.

The layers include:

NuData

Device Intelligence

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



Behavioral Insights

How we type, hold a device, or move the mouse are unique to each of us. **NuData's** behavioral insights technology passively builds a profile by looking at those inherent movements made by a user without prompting any challenges. This profile is compared against past events to analyze events in real time and help clients accurately determine if the right person is behind the device.

Mastercard Trust Consortium

By gathering and analyzing anonymized data from opted-in providers, the Trust Consortium is the world's largest network to assign risk scores to online events in real time. It uses historical risk factors, estimated trustworthiness, and reputational insights to assign a risk score to new interactions within milliseconds.

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

How does NuData work?

Every time a user interacts with the app or web platform, **NuData** passively analyzes the user's inherent digital behavior and provides clients with a risk score to make a decision in real time.

Components of that decision include:

- **Real-time scoring intelligence:** At each behavioral interaction, **NuData** generates a score array consisting of a set of behavioral scoring elements that are returned to the client environment in real time. This analysis uses intelligence anchors such as IP, email, account, device fingerprint, and device ID to analyze current and historical behavioral interactions across the full **NuData** network to identify anomalies and solve specific client

use cases. The platform also enables clients to return real-time feedback, allowing the **NuData** models to further learn in real time.

- **Score: NuData** generates a numeric score that provides a risk value for the event profiled. The score is built with data that includes behavioral observations and deviations from expected behavior. The client decides what level of risk they want to place in each score band depending on their risk tolerance.
- **Real-time evaluation and customization: NuData** has a set of rules built for each use case that are deployed with the platform. Either the client or **NuData** can propose to add or modify the rules to customize them further.
- **Real-time policy enforcement: NuData** can facilitate real-time policy enforcement through the **NuData** policy enforcement engine. It can dynamically display interdictions such as an SMS, Push to Mobile, or bot-challenges, among others. Along with providing the full mitigation solution, **NuData** can intelligently alert when in-house client interdiction enforcement policies should be triggered.
- **Intelligence dashboard:** The dashboard gives user-friendly visualization of the state of the client's traffic at any given time. The client can look at specific insights, such as the key bot characteristics from an attack and the main challenge recommendations from the platform during a period of time. This dashboard provides a clear picture clients can leverage to assess the health of their traffic. They can also create custom reports and dashboard views.

Customer support for clients:

NuData clients have access to an integration team that supports their goals throughout the entire relationship. This team includes a data analyst and a customer success expert to help the client use the NuDetect platform to reach their business goals. Clients from every region benefit from this personalized support, a contributing factor in **NuData's** award for Best Deployment and Customer Success of the Year at the 2022 Cyber Security Global Excellence Awards.

Prior to integration, the customer success team engages with clients and maintains that support throughout the growth phase. Their key focus is identifying client pain points, success criteria, and product education. They then manage the 30-day modeling period to adapt rules and processes to the client's specific traffic and platform.

BehavioSec

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

Account Takeover

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.

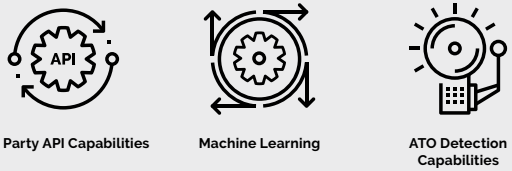
A custom ARIC model can be created for every level of potential interaction, from card issuer to acquirer, all the way to the merchant level. Further, an individual context profile is built for every customer, providing additional information for the risk models. If clients manage their own data-science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

ARIC's tiered, multi-tenancy solution provides businesses with a holistic view of their

FEATURE SPACE

OUTSMART RISK

At a Glance:



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.

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.

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.

Shape Security

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

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

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

Their primary goal for merchants is to protect against:

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

At a Glance:

User Behavior Capabilities

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

3DS & Consumer Authentication

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

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

Accertify 3D Secure

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

Accertify
AN AMERICAN EXPRESS COMPANY

At a Glance:

Accertify' s 3D Secure (3DS) Solution

Accertify's 3DS solution is available as a stand-alone authentication product or as part of their end-to-end authentication management solution. The 3DS solution supports both EMV 3DS 2.1 (3DS2) and 3DS2.2 which launched in early 2021. 3DS1.0 is now in the process of being decommissioned around the world, but **Accertify** still supports this version in regions where specific waivers were granted.

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 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, should it prove 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 third option for the issuer is to decline to authenticate. This option is used in those instances when there is an issue with the card account, or the payment is deemed high risk by the issuer's fraud solution.

Additional Protocols

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

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

- **Data sharing:** 3DS2 shares ten times as much data as 3DS1. This includes device, session, and IP data. This data enables the issuer to make better decisions when assessing the authentication request.
- **Mobile app optimization:** 3DS2 is designed to work with both a browser and app/device-based shopping experience. For example, 3DS2 can be implemented seamlessly into the merchant app, providing a much more customer-friendly experience.
- **Non-payment based authentication:** 3DS1.0 was limited to payment flows, but 3DS2 supports non-payment flows. For example, 3DS2 can be used to authenticate the provisioning of a card into an e-wallet.

- **Tokenization:** 3DS2 supports tokenized transactions, which helps to reduce the risk of the card number being compromised.
- **Support for a variety of authentication methods:** This includes one-time passcodes, biometrics, and out-of-band authentication.

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

Merchant Fraud Strategy

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

Strong Customer Authentication (SCA)

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

- Inherence (e.g., biometric)
- Possession (e.g., device)
- Knowledge (e.g., 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 newly enforced EEA regulation requirements. A merchant's failure to comply with the new EEA regulation may cause a significant number of sales to be declined by the respective card issuers.

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. **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,

Accertify 3D Secure

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 new authentication options such as Secure Payment Confirmation and Delegated Authentication. **Accertify** believes these new authentication technologies are pivotal to reducing cart abandonment.

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

Accertify
AN AMERICAN EXPRESS COMPANY

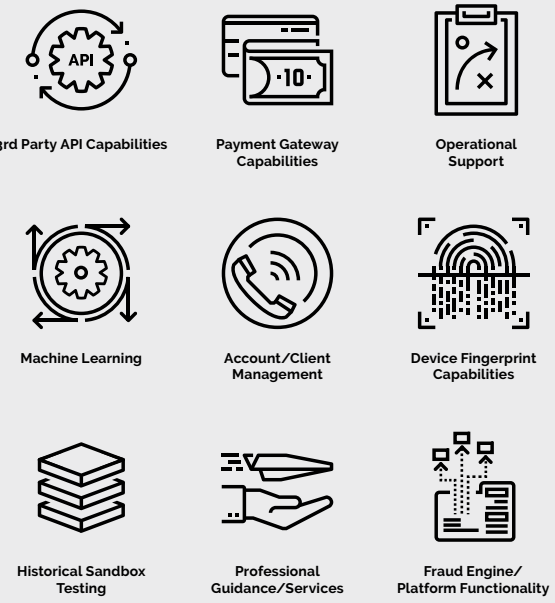
Solutions and Functionality

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

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

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

At a Glance:



Accertify, Inc.

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

In 2023, **Accertify's** Fraud Management roadmap will focus on a few key themes, including:

- Offering a new solution aimed at a variety of post-fulfillment abuses. The industry-wide surge in fraudulent and abusive requests for claims, adjustments, refunds, returns, and exchanges is a major area of concern for merchants, and **Accertify's** solution focuses on addressing those problems.
- An increased focus on account-centric views of consumers, offering visual representations of all consumer interactions for forensic and preventative analysis.
- Major investments in machine-learning capabilities, covering more use-cases and applying **Accertify's** award-winning machine learning techniques to more industries and risk decisions.
- Continued strengthening of our Digital Identity solution, addressing a wide range of risk mitigation opportunities for non-payment-related consumer interactions. Currently trained to detect bot attacks, account takeovers, promotional abuse, fraudulent account opening, deposits, withdrawals and marketplace transactions. Improved models, visualizations, dashboards and reports.
- Further distinction between fraud, policy, and abuse-driven decisions. The key to accurately measuring and assessing risk management performance is to segment these very different types of decisions.
- Additional investments in community data sets, identifying patterns of abuse that span merchants and industries, to give customers the best possible means of assessing new customers, compromised accounts, and good customers.
- Ramping up FIDO-based authentication solutions. FIDO offers an industry-standard, user-friendly, single-step, multi-factor authentication that can help distinguish trusted customers and imposters.
- Continued evolution of industry specific models, enabling merchants to automate fraud risk decisions and reallocate internal resources to focus on first-party abuse.

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

Accertify, Inc.

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

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

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

Core features include:

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

InBrowser provides JavaScript collectors that can be incorporated into any relevant web page to access detailed browser session information. Hundreds of attributes can be collected and analyzed to produce a persistent device identifier and identify potentially fraudulent behavior. Collector code can be invoked upon page visit or tied to specific actions, such as Form Submit, based on technical and business requirements. Examples of pages where

data collection is typically enabled include account open page, login page, account change/update page, and checkout/payment page.

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

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

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

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

Profile Builder: Profile Builder helps identify real-time patterns and trends through the dynamic summarization and aggregation of data. Gain insight in real-time at the transactional level to discern fraud rates, track new product launch limits, monitor account usage, analyze customer buying patterns, and uncover organized fraud rings. No longer is it necessary to anticipate potential risk, wait overnight for

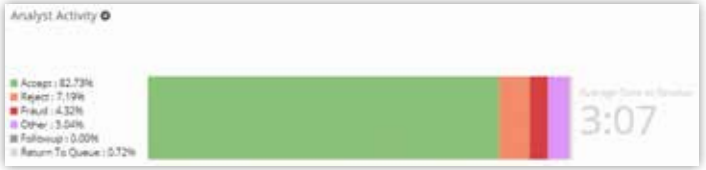
a model or algorithm to be updated or calibrated, or have static, stale rules. In real time, Profile Builder monitors summarized fraud rates at the product/sku level, across airline route networks, at events/locations, against a specific entertainment genre, or any number of similar entities. This eases manual review rates and enables a more efficient and flexible strategy to mitigate risk.

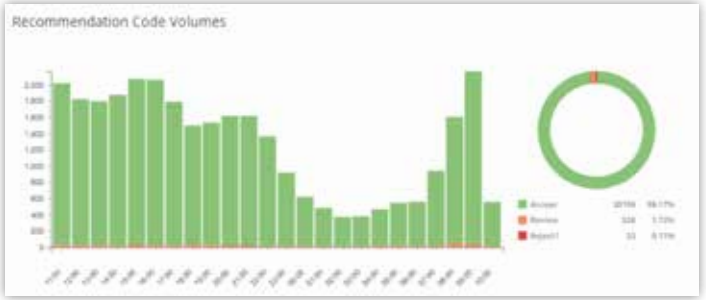
Chargeback Management: Please see full write-up in the **Accertify** Chargeback section of the Paladin Vendor Report.

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

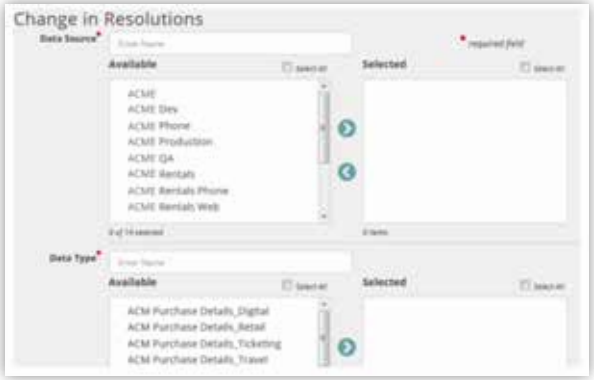
Reporting:

Accertify offers three types of reports:





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



- **Enterprise Reports:** These allow a client to input criteria parameters to specifically drill down and show different

types of performance. Examples include monetary metrics, chargebacks, analyst decisioning, rules performance, and more.

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

Refund Abuse

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

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

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

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

Accertify, Inc.

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

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

Services Offered:

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

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

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

Client Success Managers have a deep understanding of the **Accertify** Fraud and Chargeback Platform and understand how it can be deployed to solve complex challenges. The team stays closely aligned internally to ensure clients are aware of new features and functionalities and work with their client base to achieve the maximum benefit in their own environments. **Accertify** Client Success Managers are the conduit into their entire organization, standing by each client's side to guide, grow, advise, and service them as they navigate the complex world of fraud and chargebacks.

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.

Accertify, Inc.

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

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

ACI Worldwide (ACI Fraud Management)

ACI supports global fraud teams in their efforts to manage risk in a rapidly expanding digital payment ecosystem. In addition, the platform helps organizations balance conversion against fraud prevention while protecting the customer experience.
ACI understands the challenges of fast checkouts, at scale, across multiple distribution channels and payment methods. It is also not just a challenge for merchants, either—acquiring and issuing Banks also face the same issues. With real-time payments becoming mainstream and entering the merchant space, the need to understand the customer's digital identity is front and center.

ACI Worldwide is committed to innovation and continuous solution enhancement through significant investment in research and development. This ensures that the company's technology, services, and advice continue to provide demonstrable benefits to its customer base of over 80,000 merchants and 19 of the 20 top banks in the world.

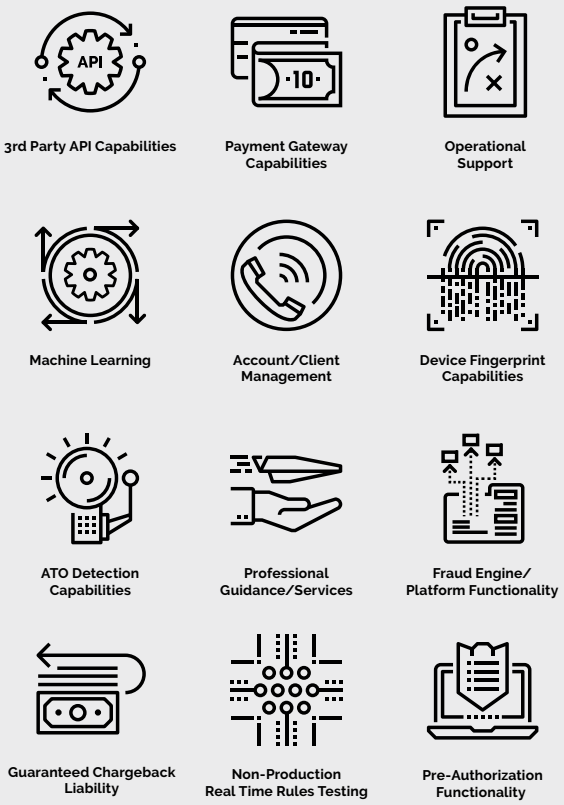
For banks and financial institutions, **ACI** customers increase collaboration across teams such as AML, card fraud, online fraud, wire fraud, and internal fraud to better consolidate overall fraud management processes while detecting signals and accessing data from multiple channels.

ACI Fraud Management for Banking

ACI Fraud Management for Banking, powered by sophisticated machine learning, supports financial institutions' ability to fight fraud and money laundering across the enterprise. While powering anti-financial crime action globally for 1 billion consumers, this represents the **ACI** flagship solution for contextual risk analysis for authorized and

ACI Worldwide
Real-Time Payments

At a Glance:



ACI Worldwide (ACI Fraud Management)

unauthorized transactions and delivers against increasing regulatory and customer demand.

Available on-premises or in the private or public cloud via a monthly subscription plan, **ACI** Fraud Management for Banking is flexible, scalable and inclusive. With 15+ years of hosted experience, **ACI** provides, manages, and implements a clients solution in Azure, allowing organizations to focus on the business of fighting fraud.

With enhanced risk management, banks and financial institutions can take control of scams, card, 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 with MoneyGuard to help combat scams, or provide frictionless protection to remain top of wallet.

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

- **Machine Learning:** Fraud scoring services. Stay ahead of real-time fraud with fully-managed, automated fraud scoring services driven by **ACI's** patented incremental learning capabilities deployed in the Microsoft Azure public cloud via an API.
- **Democratized Machine Learning: ACI** Model Generator. Democratize machine learning by taking full control of adaptive machine learning models and deploying them within hours.
- **Collaborative Machine Learning: Network Intelligence.** 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.

ACI Fraud Management for Merchants

For merchants, **ACI Worldwide** delivers fully outsourced real-time payment and fraud orchestration, enabling optimal payment journey and real-time fraud strategy, leading to an increase in approval rates, reduction in fraud, and costs of managing fraud.

ACI has a team of experts (Payment Optimization Specialists and Data scientists) on hand to advise its customers as an inclusive service offering .

Other tools available include Transaction Risk, Behavioral analytics, Chargeback Orchestration guarantee, and revenue optimization tools. They reduce both friction and operational cost for all payment methods, channels, delivery methods, sectors, devices, and globally for merchants and intermediaries.

ACI Worldwide (ACI Fraud Management)

ACI Fraud Management for Merchants enables **Fraud Orchestration** 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. The Digital Identity Services solution maximizes business growth by reducing the threat of ATO and Synthetic fraud—and providing merchants assurances of consumers' digital identity.

The technology has the ability to detect, orchestrate, and utilize over 10,000 data signals from multiple sources that enable a consumer's digital identity to be validated. Digital Identity Services enables automated decisioning to optimize revenue. 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. Features include:

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 a holistic real-time fraud prevention.

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

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

ACI Worldwide (ACI Fraud Management)

ACI Fraud Management:

A fraud orchestration technology in detail

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.
- **Incremental Machine learning:** 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.

- **Network intelligence and 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

ACI Worldwide (ACI Fraud Management)

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 call outs:** 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.
- **Smart 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 into the overall core strategy and influence final decisions.
- **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, strategy, 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:** This controls and qualifies calls to third-party value-add solutions while managing costs.

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

- **ACI Fraud Management Consultancy for banking: ACI's** Fraud Management 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.
- **Strategy and Payment Optimization Specialist for merchants: ACI**'s global team of dedicated specialists are a part of the **ACI** Fraud Management service. Analysts cover four continents (and 15 languages) and have access to global payments intelligence and local market knowledge. They have an average of five years of experience, and many are certified ecommerce fraud professionals. All have degrees in math, computer science, or data science. At the start of an engagement, risk analysts collect in-depth merchant background information, including historical fraud data. They review existing processes and operations and identify a potential strategic approach.
- **Manual order review for merchants:** Merchants are provided a team of analysts to validate and authenticate challenged transactions for a final decision of Approve or Cancel. Decisioning accuracy is tracked and monitored to ensure key performance indicators are met, averaging a 99.99% rate. Service can be deployed during season peak periods, weekends, or daily.
- **Chargeback Defense for merchants:** An **ACI**-outsourced process for chargeback and dispute management. Merchants can utilize the service to manage all chargeback disputes, including collation and submission of evidence to support the dispute application.
- **Data Scientists for both banking and merchants: ACI's** dedicated team of data scientists bring decades of experience, and are all educated to MSc and PhD level. The team is responsible for both AI and machine-learning strategies across **ACI's** portfolio. They have over 15 consortium models in production, covering all main verticals from retail to clothing, gaming, and travel. The team continues to innovate, bringing new technology to market, preventing fraud, and helping customers utilize machine learning in a meaningful way. The team is multilingual, with representation in the US and Europe. Academically, the team is well published, with over

ACI Worldwide (ACI Fraud Management)

30 publications between them, continuing to contribute to the ever-evolving domain of data science.

- **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.

Integration Process

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

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

In development over the next 12 months

Behavioral Analytics will allow 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.

ClearSale

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

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

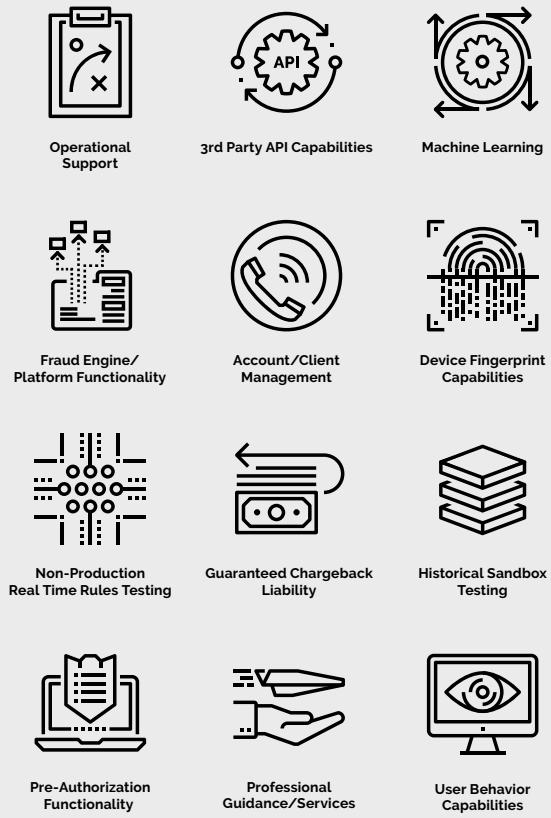
False Declines Cost More Than Fraud

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

At a Glance:



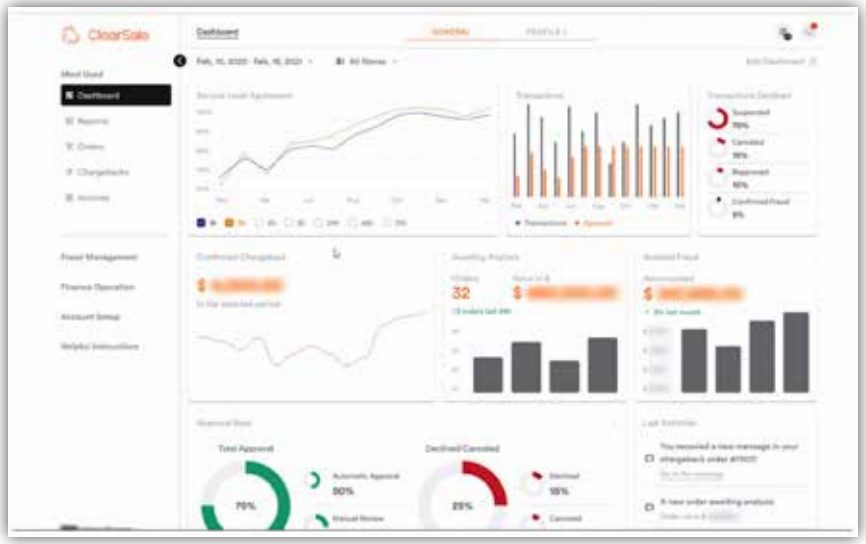
ClearSale's focus on false declines.
Most automated fraud programs are built on fraud scoring and fraud filters designed to catch and auto-decline any order the program thinks might be fraudulent.

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

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

As a result of this balanced, comprehensive process, businesses will experience reductions in decline rates and improvements in approval rates.

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



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

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

In this approach, **ClearSale** provides the full breadth of its ecommerce fraud prevention services to ensure all fraudulent

orders are blocked and chargebacks are not generated. However, **ClearSale** does not directly reimburse for any chargebacks that may occur, and the discounts provided are not intended to fully cover any chargeback losses.

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

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

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

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

How ClearSale Works

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

ClearSale does this with a multi-focus approach: a proprietary A.I. that spots every red flag and questionable action, combined with an advanced secondary review process that ensures only truly

fraudulent orders are declined.

First, a customer places an order.

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

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

Next, the A.I. technology gets to work.
ClearSale's proprietary statistical algorithm scans every order to detect common fraud patterns. Using fraud rules created specifically for the business and bolstered by a machine learning platform, the algorithm adapts to the unique fraud risk profile.

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

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

Finally, if an order is flagged as suspicious, it is sent for secondary review.
Because suspicious behavior doesn't always mean an order is fraudulent, **ClearSale's** fraud specialists are trained to look for reasons to approve orders — not decline them. Once sent through our secondary review process, if the specialist reviews the evidence and determines the order is legitimate, the order is approved.

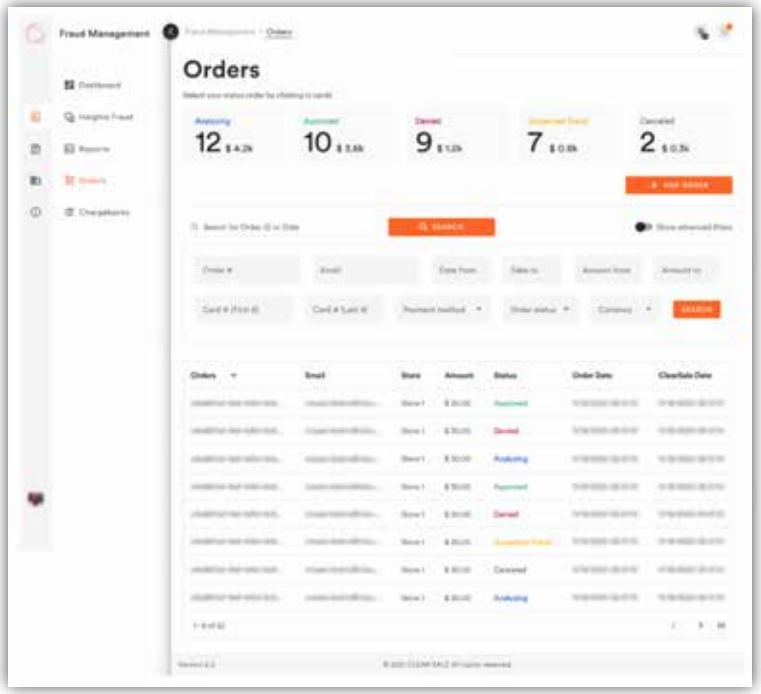
If the evidence suggests the order might be fraudulent, it is sent for a third advanced review. From there, the A.I. reviews the data elements used to calculate that transaction's fraud score, such as:

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

With that analysis in hand, an in-house fraud specialist will then gather additional insights that may go unidentified by the technology, but will provide valuable clues and consider the nuances that we see as human beings. These can include:

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

If the second or third review determines that the order is legitimate, the order is immediately approved. If the the order still cannot be validated, only then would it be declined.



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

Ecommerce Platform Integrations

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

Cybersource

Cybersource provides a cutting-edge combination of automation and customization for unprecedented control over both fraud and revenue, all backed by the strength 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 prevention 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 can solve beyond merchant fraud and traditional industries. It can support any vertical, including retail, ecommerce, transit, telecommunications, restaurants, airlines, insurance, and utilities.

The **Cybersource** and **Visa** ecosystem provides 141 billion transactions per year of insights. Each one provides insights to optimize fraud prevention, capture more revenue, and improve authorization rates. Its systems are built on proven Visa-grade systems, so data is secure.

cybersource
A Visa Solution

At a Glance:

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

Cybersource

Decrease manual review by 25% or more with machine learning

- Advanced AI resolves nearly all Decision Manager transactions and continues to migrate more and more merchants toward full automation.

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.
- 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. No waiting or status timers – instant decisions to 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. With deep customization options and a robust reporting suite, Decision Manager is ideal for enterprise business and merchants who desire refined control over their sales and fraud strategies.

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.

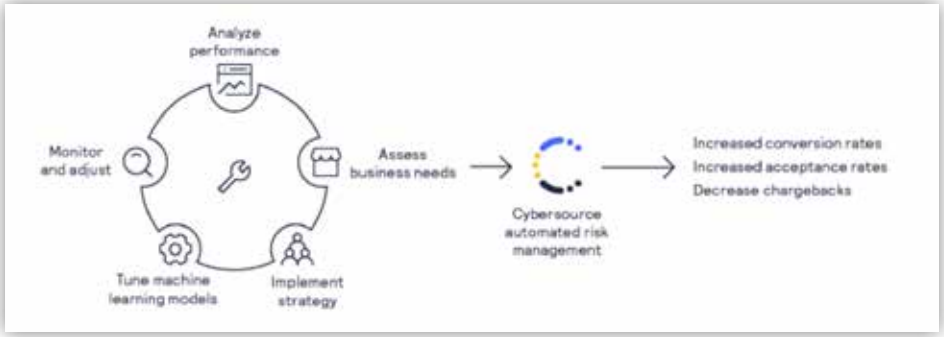
Cybersource

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 want to automate their 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 guaranteed 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.



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.

A complete suite of solutions

Decision Manager Replay

Decision Manager Replay creates a safe zone for clients to test new fraud strategies without impacting the customer experience.

Machine Learning

Based on more than 160 billion transactions annually, **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.

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

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.

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

Transaction Management
Direct access to review and investigate individual transactions.

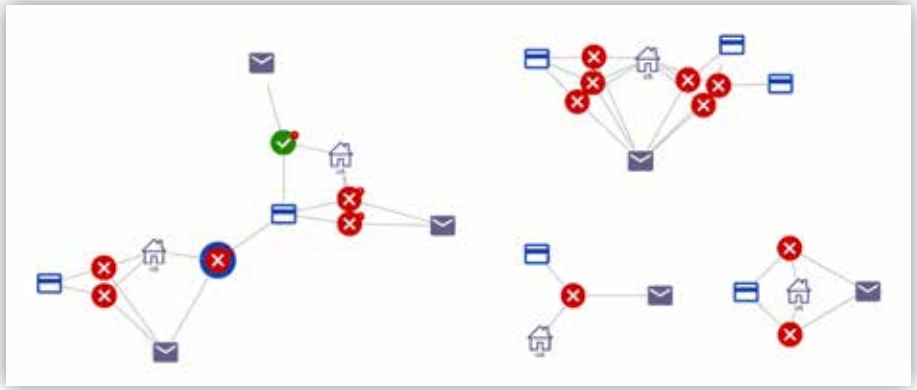
Customization
Highly-refined customization allows businesses to fine-tune their fraud strategy to their chosen level of detail.

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

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 matching to all global sanctions and denied parties lists. This provides knowledge and certainty around risky customers, even to businesses not required to connect to these lists by regulation.

Cybersource



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.

Managed Risk 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 makes 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, reduce operational costs, and increase acceptance in a balanced, business-centric way.

Pricing Model

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

12-month Road Map

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

Experian

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

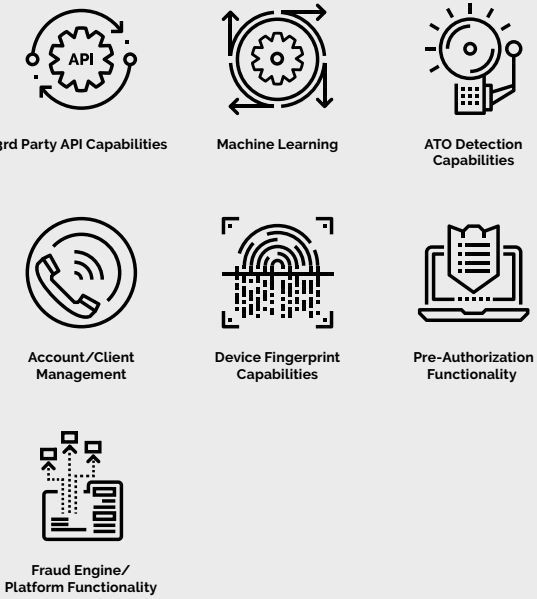
The solutions utilize **Experian**-owned consumer data, commercial entity data, device intelligence data, and a network of specialized partner solutions that cover a range of alternative data, email intelligence, phone intelligence, and behavioral biometric signals. The platform enables data assets to be combined 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

At a Glance:



Solutions and Functionality:

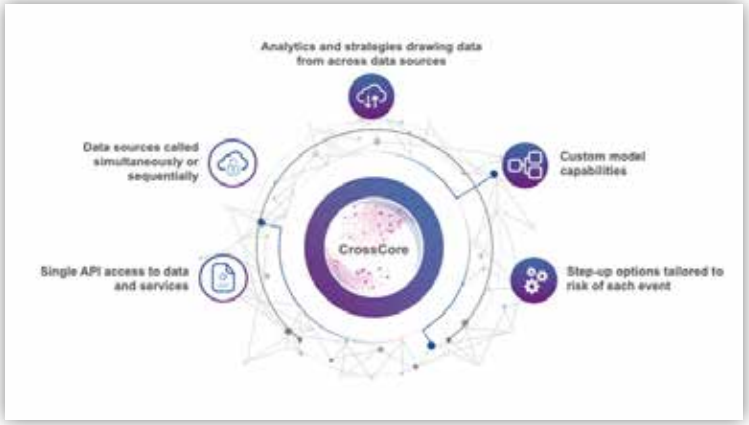
The **CrossCore** platform was built to enable clients to have full control over their identity and fraud rules and strategies through a browser-based User Interface (UI). **Experian**

identity and fraud personnel partner with the client to build the initial ruleset, models, and analytics to meet the client's requirements and apply **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. 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.

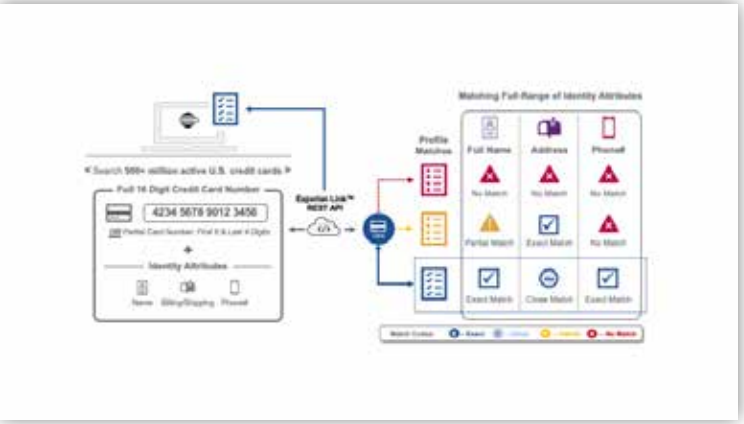
Experian Link enhances credit card authentication for the merchant by linking the payment instrument with the digital identity presented for payment. This service matches each identity attribute presented by the consumer with attributes on file with the card issuer and enhanced attributes across **Experian's** 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.
- **Disbursements and deposits:** Verify credit card ownership before accepting or releasing funds.

- **Changes to existing accounts:** Prevent account takeover by assessing updates to existing delivery or contact information.



Reporting options available:

Experian solutions offer performance and management reporting capabilities. The preconfigured reports help 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 would 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. Connect directly to the platforms using a JSON-based API, access solutions through a web UI. And utilize connectivity 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

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.

Kount, An Equifax Company

Kount joined **Equifax** in early 2021. Midigator, a chargeback technology company, then also joined forces in 2022. 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 Identity Trust Global NetworkTM delivers real-time fraud prevention and account protection. It enables customer experiences for more than 9,000 brands and works with over 50 payment processors and card networks. Linked by **Kount's** award-winning AI, the Identity Trust Global Network analyzes signals from 32 billion annual interactions to personalize user experiences across the spectrum of trust—from frictionless experiences to fraud blocking. Their Identity trust decisions focus on delivering safe payments, account creation, and login events while reducing digital fraud, chargebacks, false positives, and manual reviews.

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

By combining both forms of machine learning with the Identity Trust Global Network, **Kount** can provide trust or risk decisions in real time. Unsupervised machine learning

Kount®

At a Glance:

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** Identity Trust Global Network, which includes billions of transactions from over 14 years of data in over 250 countries and territories, as well as more than 50 payment and card networks.

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

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

Products

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

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

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

Kount Command gives customers access to the Identity Trust Global Network, which includes adaptive AI. **Kount's** AI combines supervised and unsupervised machine learning to detect existing

and emerging fraud. **Kount's** unsupervised machine learning doesn't require historic data, which can help businesses adapt to changing consumer demands.

Kount Command automates fraud detection, detecting common, sophisticated, and previously unknown fraud attempts in less than 250 milliseconds. **Kount** also allows for flexible control, with a customizable policy engine. Customers can fine-tune fraud prevention decisions, conduct investigations, and monitor performance. They can create policies that meet their unique business needs and customize risk thresholds to address emerging attack methods and new use cases.

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

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

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

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

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

Kount, An Equifax Company

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

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

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

Partners

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

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

Kount, An Equifax Company

Features and Functionality

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

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

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

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

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

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

Professional Services

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

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

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

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

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

Kount's Consulting Services 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.

Riskified

Riskified works with many of the world's largest merchants and prestige brands to maximize ecommerce revenues by minimizing fraud and policy abuse. **Riskified's** advanced machine learning platform is designed to lift approval rates, increase authorization rates, prevent policy abuse, secure against account takeovers (ATOs), and optimize payment flows. **Riskified** also pioneered a full chargeback guarantee coverage to empower merchants to grow their business safely and with complete confidence.

Benefiting from a sizable team dedicated to global fraud research 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 over $1 billion in gross merchandise value (GMV) from over 180 countries in 2022.

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

Solutions and Functionality:

Chargeback Guaranteed Fraud prevention

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

At a Glance:

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

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

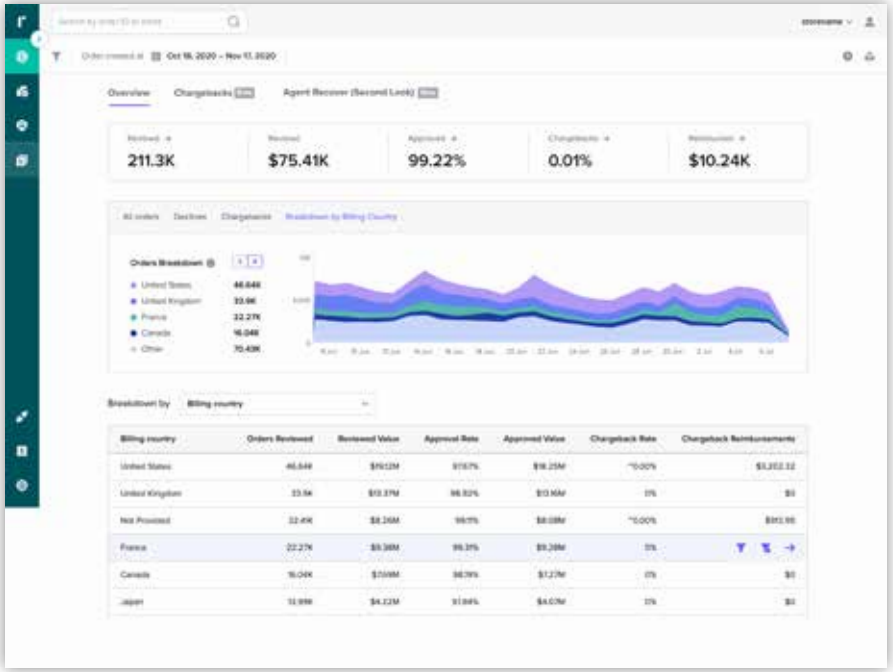
In addition, the platform provides context for every decision and provides support teams and fraud teams with dedicated tools. Agents and leadership can use the provided Control Center to track performance or dive into the data to analyze fraud and payment trends.

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

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 driven 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.

Riskified



Policy Protect:

For organizations that maintain certain 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.

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.

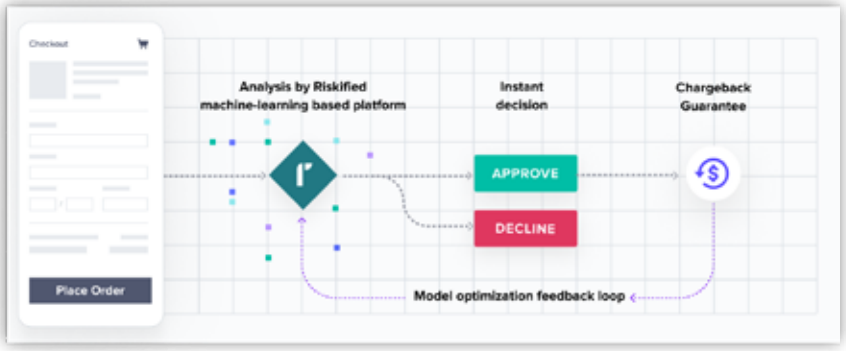
Identity Explore:

Identity Explore, a revolutionary new capability, allows 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.

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.

Riskified



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 and partners can integrate with **Riskified** via API integrations and/or various ecommerce platforms and plugins available. Flexible integrations will allow better fitting for various platforms and architecture in use by the merchant. For chargeback guaranteed fraud prevention and optimization, for example, merchants can trigger **Riskified** pre- and post-payment authorization.

Most of the integration effort is handled by **Riskified's** internal teams, with support from the merchant. A typical Riskified integration takes between 6-10 weeks, including the integration itself and shadow mode – where **Riskified** is receiving live orders but the merchant is not acting upon the decisions. This is intended to calibrate machine learning models and ensure performance from day one.

Riskified can provide synchronous guaranteed decisions in under one second (P99). Pre-authorization optimization recommendations can be provided in under 0.5 seconds (P99).

And a typical fraud prevention analysis response time distribution (from certain integration setups) is 600ms, with a median response time of 400ms (P95).

Additionally, **Riskified's** strategy to expand into new geographies includes select "white labeled" partnerships with well-established payment gateway, acquirer, and PSP platforms. For example, throughout LATAM, there are four integrated partnerships that resell the chargeback guarantee offering, powered by **Riskified**. Each of these partner relationships have expertise in specific industry verticals, like gaming, travel, ticketing and money movement. This strategy was first launched in EMEA with well branded partnerships like Axerve and has also extended into APAC, with Novatti, and NTT Data to name a few.

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.

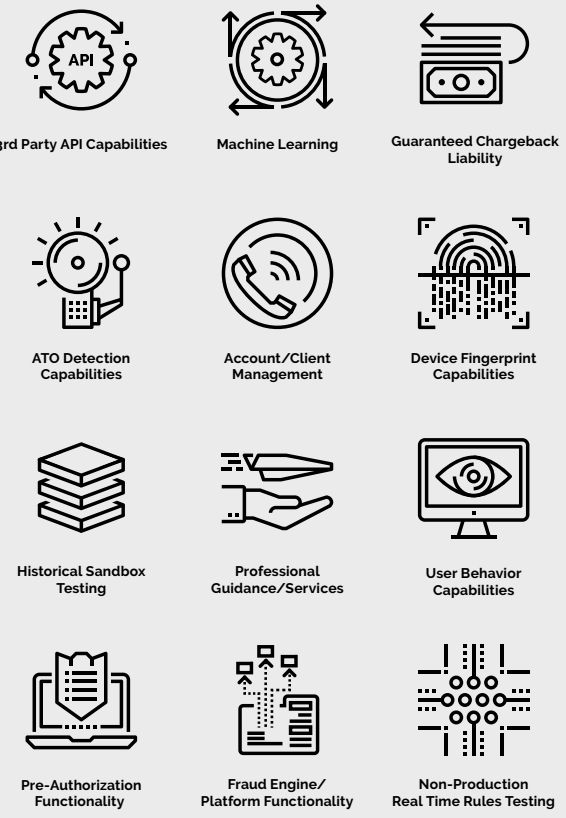
Handling 960 million transactions per year totaling over $150 billion, their volume is growing by 5-10% every month. They support clients' goals by focusing on fraud loss rates, fraud prevention program operating expenses, approval rates, account takeovers, suspicious AML activity count, and payment 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:

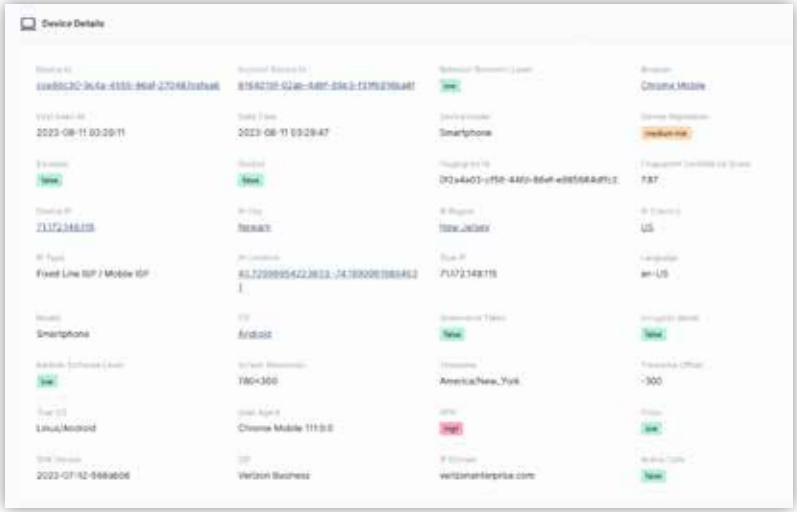
- Sardine offers a compliance solution that includes sanctions screening and monitoring services for individuals and businesses, crypto wallet screening, AML transaction monitoring services, and case management.

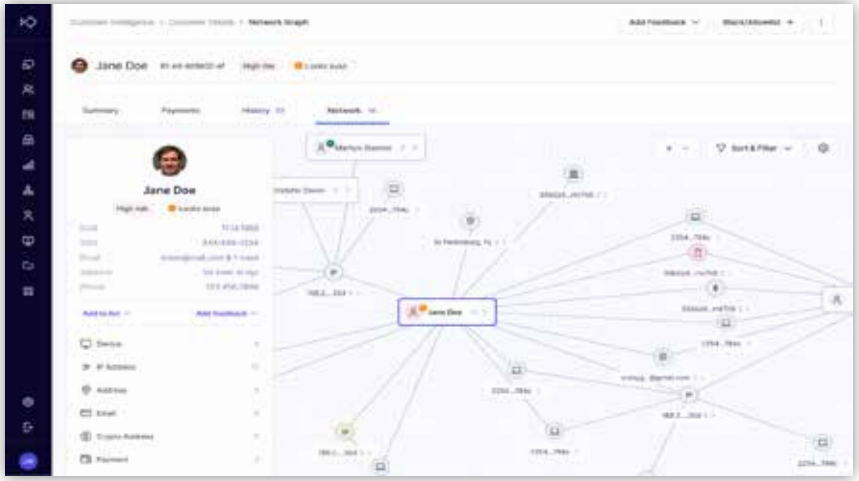
Sardine

- 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.

Sift is a leader in digital trust and safety, empowering businesses to unlock new revenue without risk. **Sift** dynamically prevents fraud and abuse with real-time machine learning, a global data network of 70 billion events per month, and a commitment to long-term customer partnerships. Global brands such as DoorDash, Twitter, and Wayfair trust **Sift** to lower chargeback rates, proactively prevent online fraud, and fuel business growth.

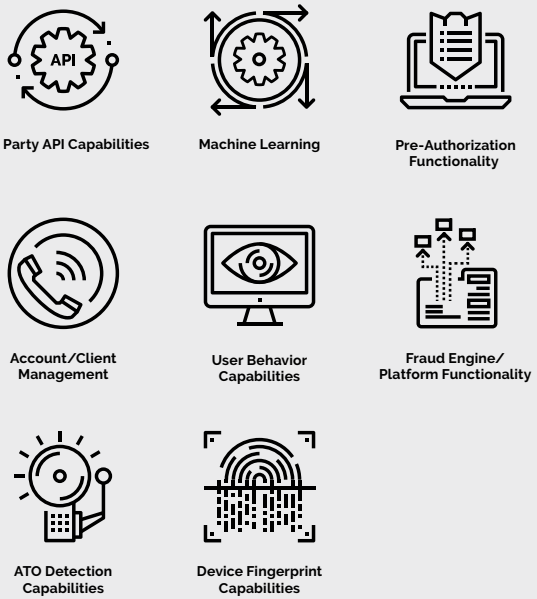
Solutions & Functionality

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

Based on these events, **Sift** assesses the risk of account creations, logins, orders, user-generated content, and unique events 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

At a Glance:



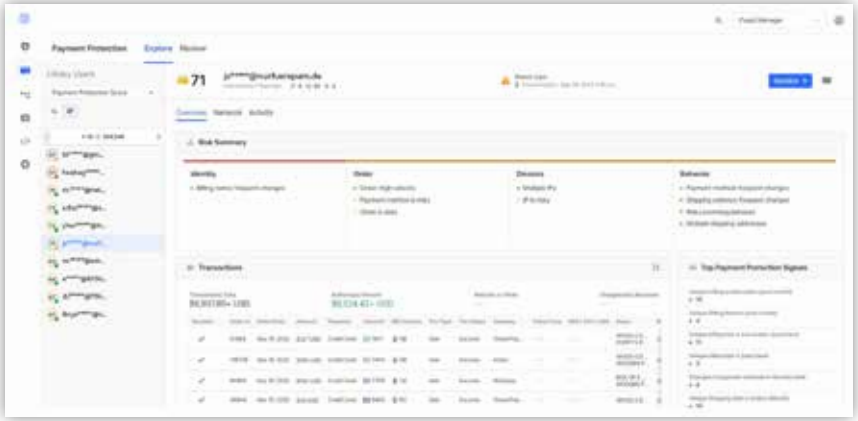
unique to them. **Sift** also performs extensive feature engineering on individual data elements to generate tens of thousands of signals across identity, device, behavioral, and transaction vectors.

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. The Console gives trust and safety teams of all sizes a platform designed to investigate fraud patterns, automate decisions, conduct manual review, and analyze business performance. It also supports capabilities for multi-factor authentication and decision optimization as well as false-positive experimentation.

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

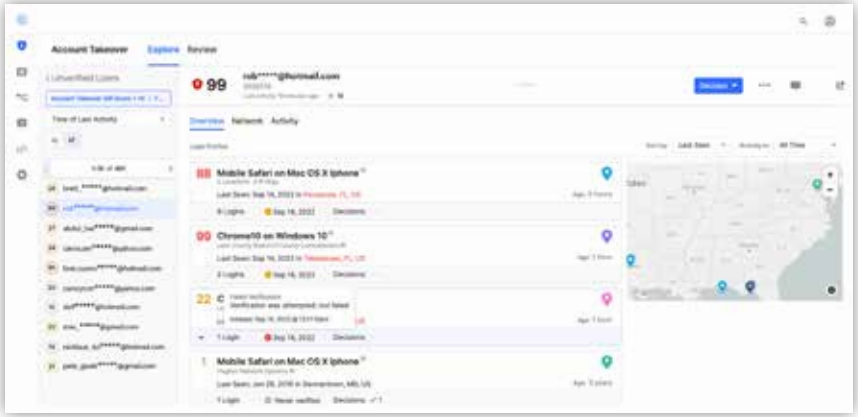
Payment Protection

- Proactively address all types of payment fraud, including fraudulent chargebacks, to protect revenue
- Block fake accounts and risky signups
- Streamline operations and reduce time spent on manual review with case management, automation, and reporting



Account Defense

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



Content Integrity

- Proactively address spam, scams, and other malicious content
- Mitigate inauthentic or duplicate accounts and risky signups
- Build automation, review risky cases, and remove malicious content at scale

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

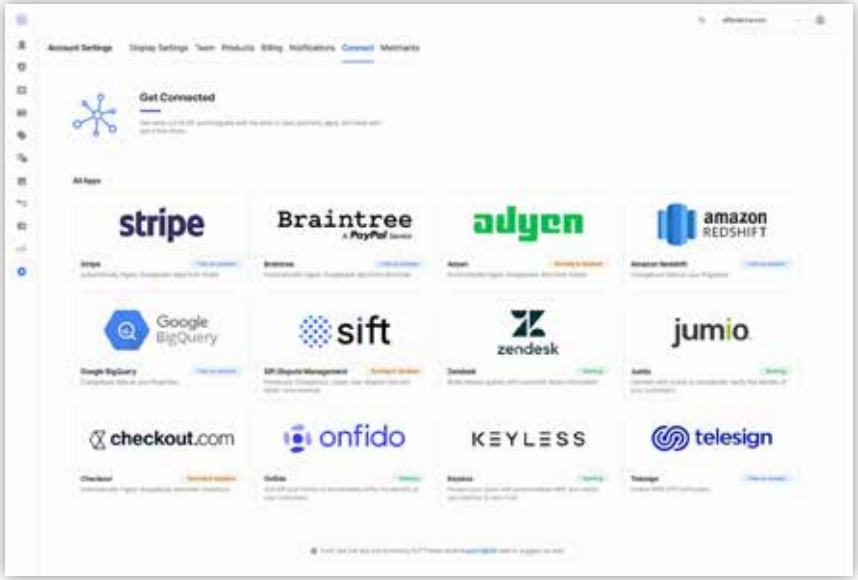
- **Case management and network graph: Sift** provides machine learning insights in a visual interface, so analysts can understand the reasoning behind each **Sift** assessment and expedite manual review decisions. This includes risky signals, locations of IPs, order and content history, and a network graph that shows signals shared across multiple users.
- **Manual review queues:** Customers can queue users, orders, or content for manual review based on customizable criteria that leverages the **Sift** Score and other fraud signals. Queues automatically assign open cases to individual analysts, while avoiding overlapping reviews. These queues also support escalation for additional rounds of review by senior analysts or managers.
- **Automated Workflows:** Trust and safety teams can automate decisions and business processes by defining automated Workflows based on criteria using "if/then" analysis. Workflows are completely customizable and can be, for example, configured to automatically reject risky sessions, reduce friction for trusted users, assign transactions to analysts for manual review, and initiate additional verification processes such as 3D Secure and SMS verification.
- **Customizable roles and permissions: Sift** supports multiple user types with a wide range of permissions depending on the requirements of their role. For example, admins may have access to manage Workflows, analysts may have access to order details and the ability to make decisions, and a developer may only have access to integration health information. Customers can configure custom permissions to suit their team needs.
- **Multilevel account support:** Customers can set up sub-accounts within a global account to support multiple business units and geographic regions. Sub-accounts are easy to jump between, and a global view provides aggregated insights across all sub-accounts.

- **Real-time analytics:** Admins can track business health with comprehensive insights that report on different criteria, such as order block and acceptance rates, chargeback rates, and risky signups.
- **Built-in Authentication:** Customers can set up email or SMS notifications within the Workflows environment to authenticate any risky signals or transactions that need an additional check.

Sift Connect

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

- **Low- and no-code integrations:** Trust and safety teams can integrate with **Sift** using connectors to popular digital commerce platforms, such as Adobe Commerce and Salesforce Commerce Cloud.
- **Consolidated data and tools:** Apps make it easy to ingest data from other solutions such as PSPs and third-party data providers. Once an app is installed, the data is available within the Console—reducing the number of tools analysts need to switch between to do their jobs.
- **Higher levels of transparency:** Integrating fraud data from **Sift** with other business data in data clouds and business intelligence tools enables flexible reporting.



Services Offered

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

A team of Trust and Safety Architects, all of whom are industry experts with years of in-house fraud prevention experience, are available for consultation to help teams of all sizes with a holistic, scalable Digital Trust & Safety strategy. Support Engineers are

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

In development in the next 6-12 months:

- Expanded Workflows/Rules capabilities, including new advanced analytics
- Advanced machine learning capabilities
- Optimized integration and tooling for the unique needs of PSPs who service several merchants across various industries
- Expanded range of authentication options
- Improved and customizable reporting capabilities

Signifyd

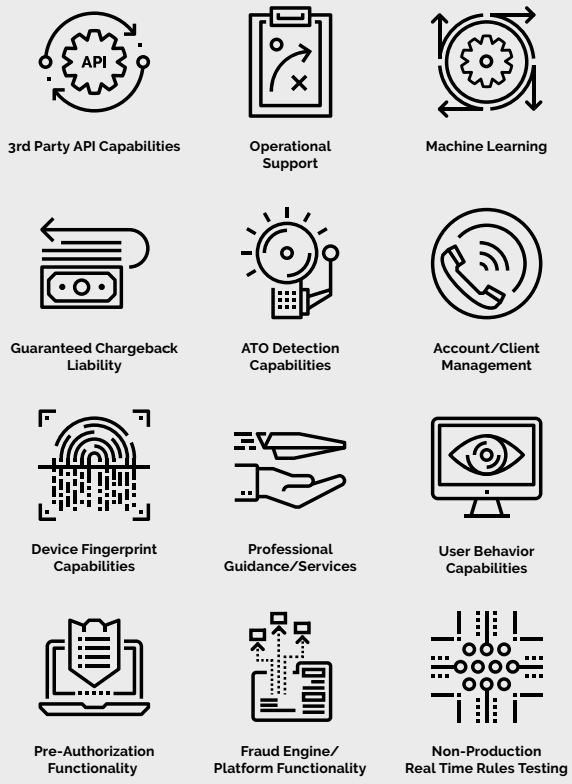
Signifyd's Commerce Protection Platform helps address fraud challenges at key conversion points across the ecommerce shopper journey from account login to return request. By eliminating fraud and abuse throughout the funnel, the platform allows merchants to protect revenue, trust customers and promote growth. **Signifyd** has been ranked No. 1 Payment Security and Fraud Prevention vendor in Digital Commerce 360's Retail Top 1000 for the last two 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.

Signifyd

At a Glance:



- **Grow "Fearlessly":** Chargeback liability often leads to decisions made by fear of loss. By shifting liability away from ecommerce merchants, **Signifyd** helps eliminate the roadblock of fear to enable fearless growth. The platform allows merchants to more confidently launch new products, expand internationally, offer omnichannel shopping experiences, and establish flexible business policies and customer rewards.

Platform, Solutions & Functionality

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

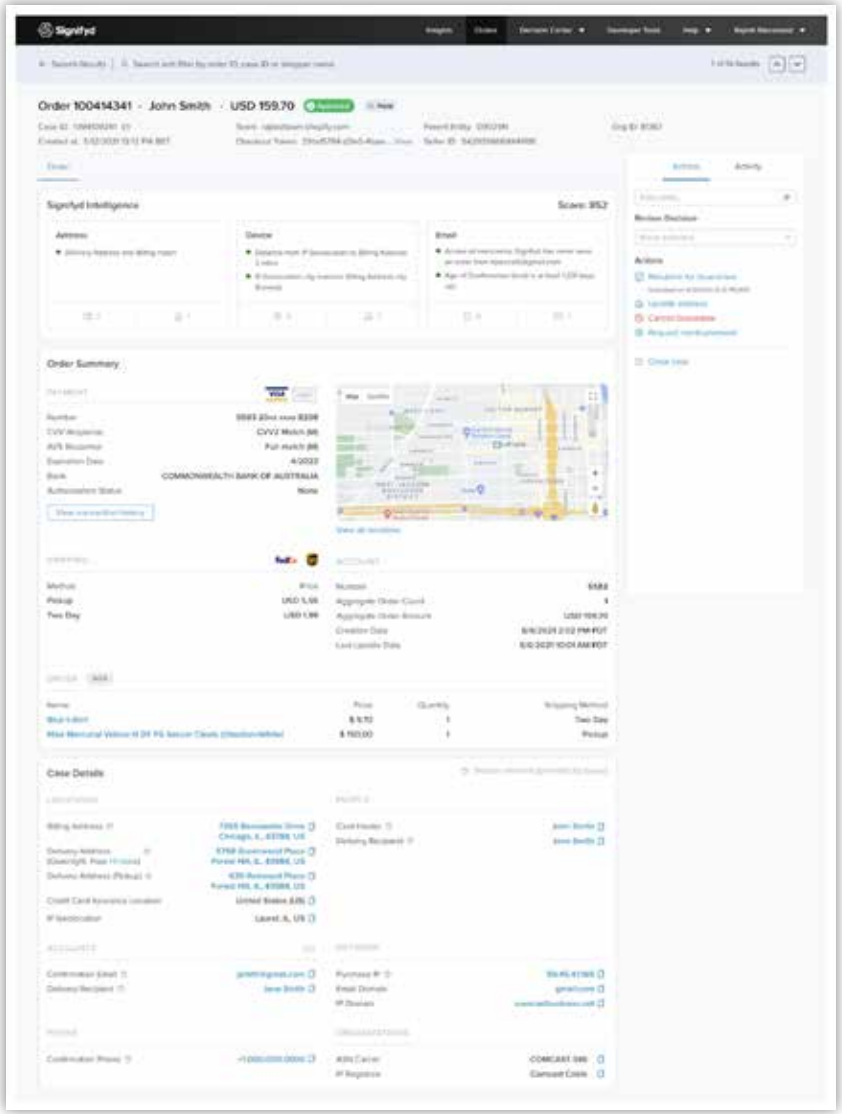
Signifyd's Commerce Network: As the foundation of the Commerce Protection Platform, Signifyd's Commerce Network combines identity and intent intelligence from thousands of global ecommerce retailers with Payment Service Provider (PSP) data, issuer insights and a merchant's own consumer data to proactively 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, and **Insights Reporting** to provide the business intelligence and benchmarking necessary to optimize performance over time.

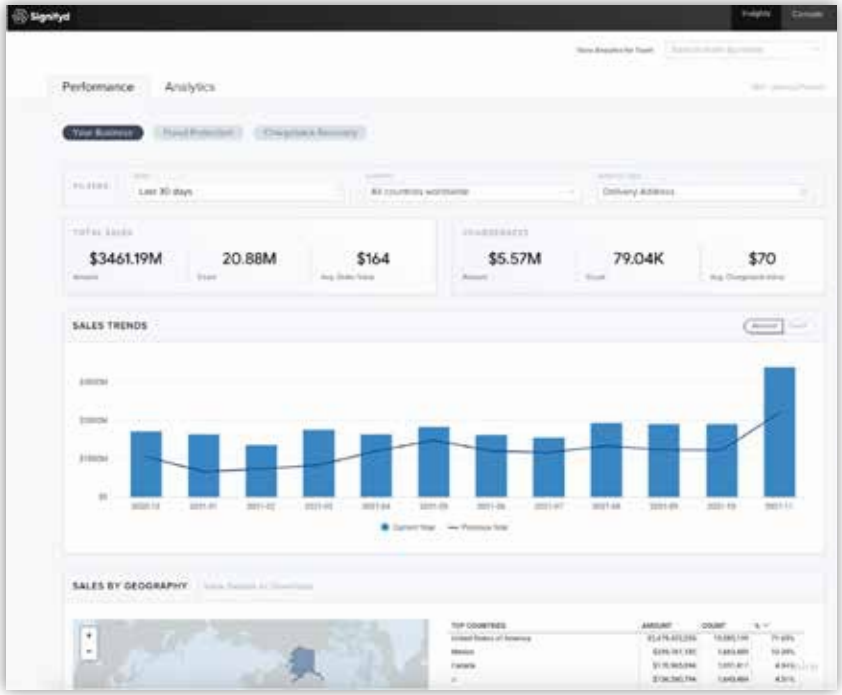
Similar to the need for transparency into decisions, merchants migrating to machine learning from rules-based platforms want to maintain control over their unique business policies and the customer experience they drive. **Decision Center** allows a risk or fraud management team to draw on network insights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



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 and interact with the data dynamically in real time.

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

- **Account Protection** analyzes behavioral and device data from login through checkout to protect customer accounts and the sensitive financial information, gift card details, and loyalty points they contain from malicious schemes and to mitigate damage posed to brand reputation. By monitoring consumer behavior across the network, **Signifyd** can help detect anomalies in shopper interactions and stop fraudulent account activity in real time.
- **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, and Shopify.

Direct API integrations require approximately three days' worth of development and testing. There are contractual service level agreements for system uptime, in addition to the redundancy that comes with hosting the system on the cloud 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 adding new issuer partners to the **Signifyd** Commerce Network to improve auth decisioning accuracy, a new integration with Narvar

to embed **Signifyd's** return abuse policies and decisioning into consumer-facing workflows, and enhancements to order search and insight visualization.

Vesta

Vesta is a transaction guarantee platform focusing on digital purchases. They support organizations in the pursuit of increasing approval rates and eliminating all costs associated with fraud. This includes direct losses as well as lost sales and false declines.

Processing over several billion dollars' worth of transactions annually, 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, eCommerce Marketplaces, and Payment Service Providers (PSPs)

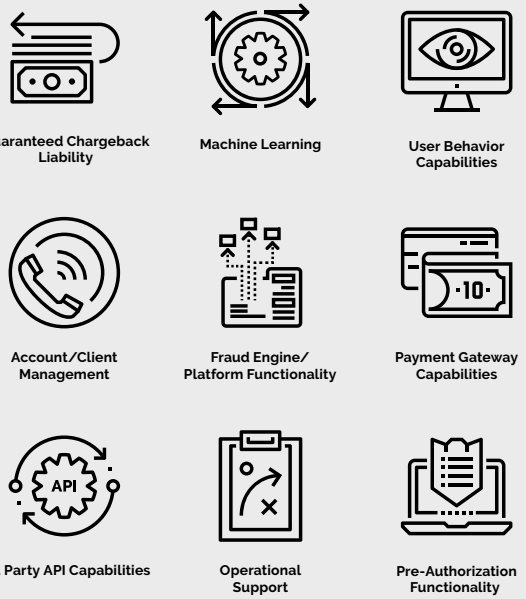
The solution helps organizations focus on a range of KPIs including:

- 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

User-friendly console

Vesta solutions begin with the customer lens – a simple set of flexible integration methods that enable deployment easily across all digital channels-- website, native applications, IVRs etc.

At a Glance:



Vesta

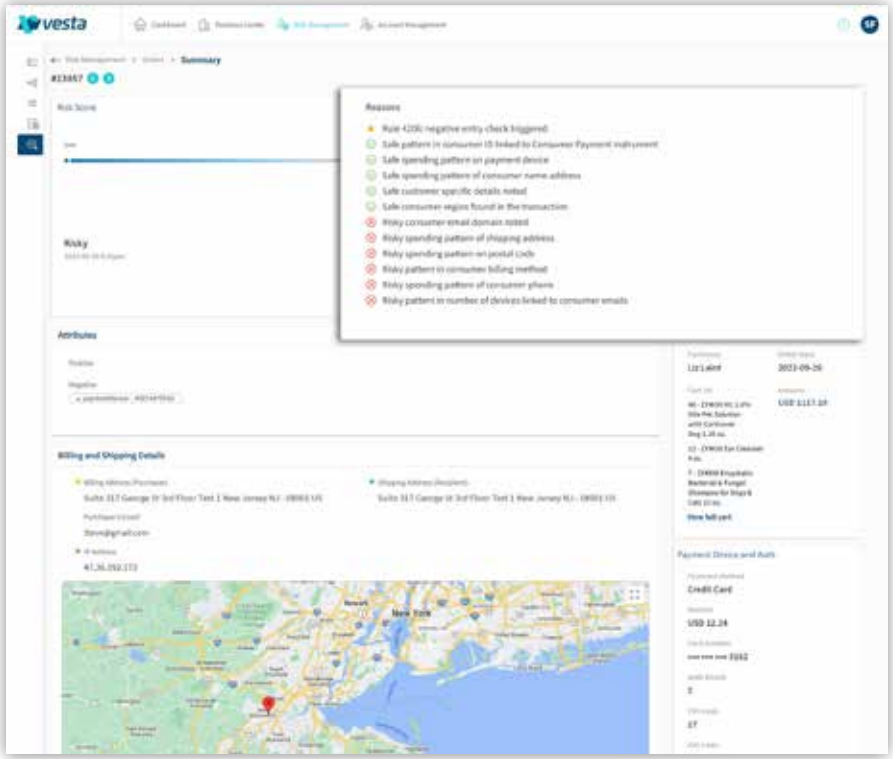
Trillions of data points analyzed by cutting-edge machine learning (ML)

The combination of global consortium data, behavioral and device fingerprint information, plus additional third-party data feeds real-time network analysis. Using advanced machine learning and artificial intelligence, Vesta establishes and analyzes linkages between incoming transactions and the entire data set that has billions of unique identities to derive patterns, detect anomalies to get the highest surety decision about the risk associated with the transaction.

Solutions and functionality:

Vesta Payment Guarantee is full-service fraud protection that guarantees decisions **against fraud chargebacks** 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. Approval rates typically increase by an average of 10%.

In this instance, **Vesta** will completely manage rules, models, and decisions for the customer through a hands-on data science team. With Payment Guarantee, any costs of fraud chargebacks drop to zero as **Vesta** covers the transaction amount plus any chargeback fees. This optimizes the customer experience and enables businesses to focus on generating revenue. The average response time for this solution is around 800 milliseconds.



Vesta

Vesta Payment Protect helps customers accept more orders with confidence, managing fraud using strong data science and an AI-driven decision engine that delivers risk assessments in less than half a second. Standard rules and models are provided and then managed by the customer thereafter. Payment Protect delivers a high-level risk indicator, a risk score, and detailed insights via risk score reasons. The average response time for this solution is around 0.5 seconds.

Reporting options available:

All products share a common web-based console tool that enables customers to view real-time information that is important for monitoring their business. This console includes a dashboard landing page that highlights the most important metrics. Other reports such as orders drilldown, chargeback management, and other configuration options are available.

Proof of Concept process:

Vesta offers two different types of POC's – offline and online. The offline POC utilizes historical data to do an A/B test. Online POC is basically a full integration to one of the services. Based on the contract, this can be set in shadow mode so the customer is not charged but can compare results against any current platform.

Pricing format:

Vesta Payment Guarantee pricing consists of a one-time fee and ongoing usage fees. The one-time fee covers onboarding and configuration. Usage fees are based on a percentage of the total purchase value of transactions that are guaranteed by the service. **Vesta** Payment Protect uses a combination of a monthly minimum with a transaction-based fee.

Integration:

Customers can choose between several options:

- Integrating through a set of API calls they would call during the transaction flows
- Using the VestaJS (Java script) library
- Insert the **Vesta** SDKs into their native mobile applications

Vesta has a streamlined integration process to help mitigate the time, effort, and complexity of integration. Customers are assigned a dedicated Integration team to assist along the way. A customer dashboard will guide them through the integration process and facilitate integration testing. The organization offers different integration options to accommodate the needs of their business. Current time from signature to launch is less than 60 days.

Vesta

Support packages available:

Currently all platform and product support are included in all contracts. No extra fees are required for support plans at this time. A 24/7 NOC for all platform-related issues is also available. Product support is handled through a ServiceNow ticketing system with service level agreements (SLAs) set based on priority.

12 Month Roadmap:

Over the coming year **Vesta** will be focusing on enabling PSPs and Gateways to more easily leverage their products for sub merchants. They will also enhance the payment protect product to offer additional capabilities and features for customers who want to use their score and insights to make their own decisions.

In addition, **Vesta** is planning more integrations with ecommerce marketplaces such as vTEX and Magento.

Apruvd

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

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

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

The service is offered in four customizable tiers:

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

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

At a Glance:

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

Arkose Labs

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

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

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

Solution highlights include:

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

Arkose Labs

At a Glance:

Fraud Engine/ Platform Functionality

Guaranteed Chargeback Liability

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

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

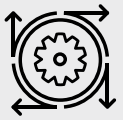
Feedzai chose not to participate in the Paladin Vendor Report at this time. If you would like to see them participate in this report during an update period or at the next annual publishing, please let us know by clicking here: info@paladinfraud.com.

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:

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

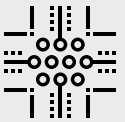
Solutions and Functionality

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.

Ravelin

The areas with full solutions include:

- Account takeover prevention
- Voucher and policy abuse
- Loyalty abuse
- Marketplace supplier fraud
- Bot detection and mitigation
- In addition to fraud, **Ravelin** also offers payment solutions which can be used to navigate PSD2 regulation. These include:
- 3DS server for PSP agnostic authentication for large merchants, up to version 2.2 exemptions management.

Radial

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

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

Benefits include:

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

Radial

At a Glance:

Guaranteed Chargeback Liability

Machine Learning

User Behavior Capabilities

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

SEON

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

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

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

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

At a Glance:

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

Simility

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

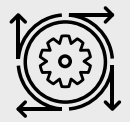
When information is added, their models will adapt and evolve to those patterns. They say the models adapt and detect patterns of fraud before they are perceptible to human analysis. Also, manual rules are arranged into code and fed into their machine-learning models.

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

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

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

At a Glance:



Machine Learning

Fraud Engine/ Platform Functionality

Device Fingerprint Capabilities

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

SpyCloud

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

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

Solution

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

SpyCloud

At a Glance:

Operational Support

ATO Detection Capabilities

Account/Client Management

Fraud Engine/ Platform Functionality

SpyCloud

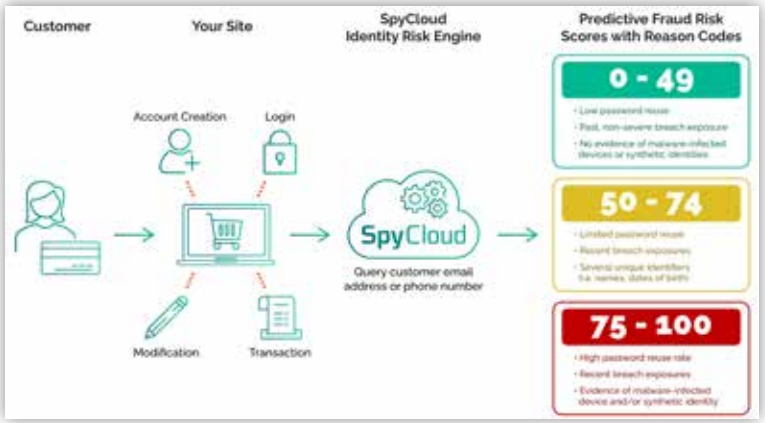
While most people have had some data exposed on the criminal underground, the fraud risk posed by that exposure varies substantially by the type of data exposed, the recency, and the method of compromise. The scores delivered by **SpyCloud** Identity Risk Engine correlate a user's multiple online personas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

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

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

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

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



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

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

SpyCloud

Primary Capabilities include:

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

The SpyCloud platform can help support the following strategies:

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

Proof-of-Concept (POC) process:

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

SpyCloud

Channels of specialization:

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

Integration

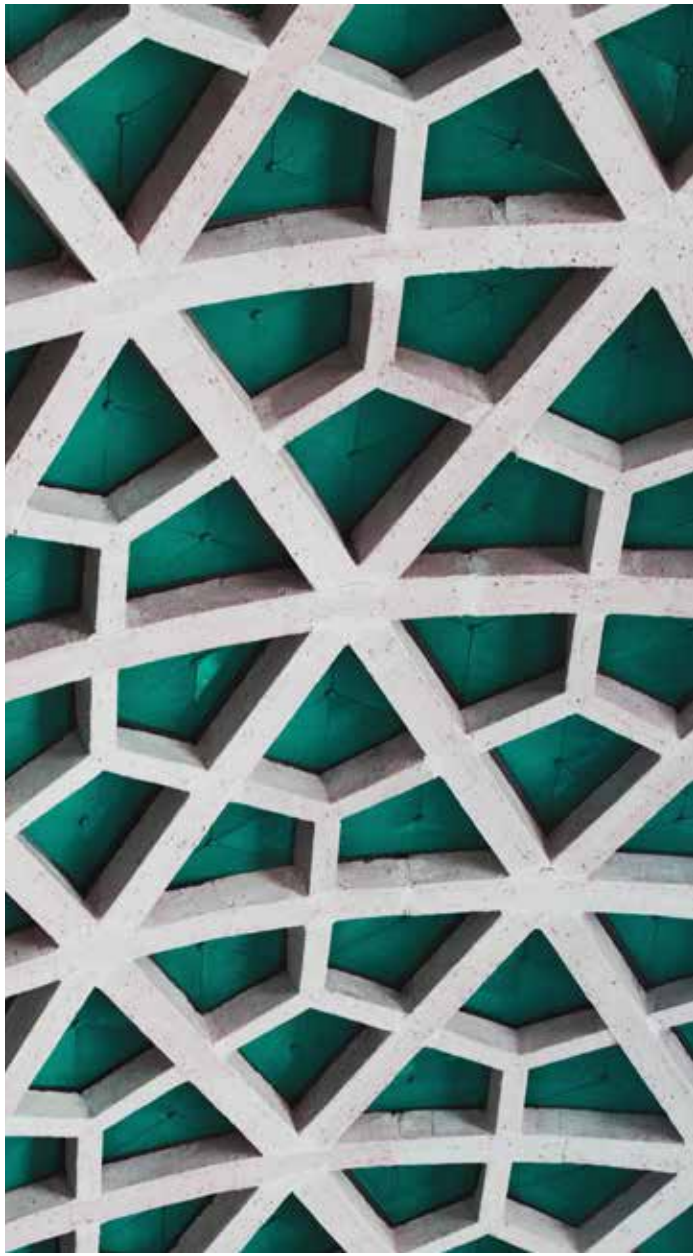
SpyCloud offers access to Identity Risk Engine via a high-volume, REST-based API, as well as via batch transmission. The API delivers sub-second response times and requires minimal effort to integrate, providing numeric and text character results for ease of ingestion. Access is also available via a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

12-month roadmap:

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

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™ orchestrates behavioral, device, and identity insights to help organizations secure trust across channels and deliver seamless experiences for consumers. This enables companies to increase trust at each stage of the customer journey and across channels to nurture deeper, more efficient, and lucrative customer relationships.

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

To **TransUnion**, "digital identity" means using a host of authoritative identity signals to quickly identify, authenticate, and fast-track legitimate customers and interactions while mitigating against the negative impact of fraud. The more accurately consumers can be identified, the harder it is for malicious users to spoof identities and take over accounts. It ultimately makes better decision-making possible and facilitates a more frictionless consumer experience.

This is achieved through the **TransUnion** identity intelligence network—a repository of online, offline, and call center data that is broken down, corroborated, and rebuilt up to every 15 minutes with updates from proprietary data sources with direct relationships, including billing, telecom, and government agencies. This identity backbone is powered

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

by an always-on network of partners, many of which are the provisioning source. The network effect of a massive marketing footprint, device consortium data, international credit data, carrier device data, and customer CRM data is a holistic view of risk identity allowing for greater accuracy and omnichannel fraud and risk insights.

TruValidate helps organizations instill trust in consumer interactions across all channels, improving customer conversions, minimizing fraud losses, and enhancing customer satisfaction.

Solutions and Functionality

TruValidate comprises four primary product offerings that protect brands from fraud losses while delivering seamless customer experiences.

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:** Strengthen fraud capture early in the digital user flow, and evaluate device reputation and riskiness to mitigate fraudulent transactions and account takeover—all without imposing unnecessary friction on trustworthy customers.

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:** Helps ensure the safe and friction-right delivery of step-up authentication, including one-time passcodes.
- **Inbound Authentication:** Improves customer experiences and speed call resolution, and reduces fraud risk by treating each inbound caller according to their trustworthiness.

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.

TransUnion

- **Identity Verification:** Welcome new customers with high confidence in their identities and minimal step-up challenges.
- **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:** Digitally authenticate official documents to reduce the risk of identity fraud while offering a convenient, digital customer experience.

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.
- **Synthetic Fraud Model:** Expedite service to legitimate customers and project the organization from synthetic fraud.

Socure

Socure is a market leader and highest valued private company in the identity verification and fraud prevention industry. Its predictive analytics platform applies artificial intelligence and machine learning techniques with thousands of sources of trusted online/offline data to verify every element of identity in real time, including government documents, email, phone, address, IP, device, date of birth, and SSN. The company offers a complete set of solutions across fraud risk, compliance, document verification, and account validation. Starting at digital onboarding and persisting throughout the customer lifecycle, **Socure's** platform provides accurate, inclusive identity verification and fraud decisions for top companies across all verticals.

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

Today, **Socure** has more than 1,500 customers, **Socure** enables trusted customer transactions across the financial services, government, gaming, workforce, healthcare, telecom, and ecommerce industries. Customers include four of the top five 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 third-party and synthetic ID fraud risk, increase auto-acceptance, and reduce false positives and friction. And they do it while optimizing the digital customer experience at application, account update, password reset, high-value transaction, and across the customer lifecycle.

Socure's graph-defined identity verification platform is built on eight billion rows of identity data coming from a combination of externally purchased data sources, network velocity, and client feedback data from the **Socure** Risk Insights Network.

SOCURE

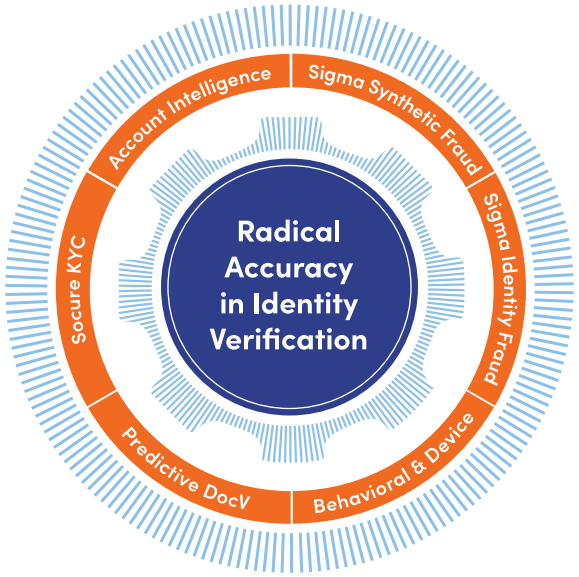
At a Glance:

- Machine Learning
- Device Fingerprint Capabilities
- User Behavior Capabilities
- Account/Client Management
- 3rd Party API Capabilities
- Operational Support
- ATO Detection Capabilities
- Fraud Engine/ Platform Functionality

Socure

Socure's fraud and identity solutions were designed and have been continuously optimized to focus on the riskiest 2-3% of applicants, drastically increasing fraud capture and reducing false positive rates in the most critical review and decline populations possible. Through this focus on accuracy, the company supports a number of use cases, both pre- and post-authorization, such as new account creation, sign-in, guest checkout, account update, and more.

Solution Highlights



Socure Risk Insights Network

The **Socure** Risk Insights Network (the Network) is at the center of the **Socure** ID+ fraud and identity 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 Identity Fraud provides a third-party fraud solution that analyzes every dimension of consumer identity through a single machine-learning (ML) model. It helps organizations maximize auto-approvals and minimize both fraud risk and false positives. And it allows organizations to streamline risk operations. The solution analyzes every dimension of consumer identity—

name, email, phone, address, date of birth, SSN, IP, device, velocity, network and behavioral intelligence, and more—in a single ML model. Sigma Identity Fraud captures 85%-90% of fraud in the top 3% of riskiest users, often reducing false positives considerably.

Socure 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.

This means 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 customer portfolio by conducting "scrubs" using synthetic fraud models.

Socure's Email, Phone, and Address RiskScores can be applied in a number of situations. Often, organizations wish to assess specific elements of an identity for further verification—for example, at password reset or account profile change. Alternatively, this can also be the case at onboarding if limited identity attributes are collected by a given consumer-facing service. **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.

Socure's identity element-specific ML 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. In addition, **Socure's** Sigma Device module verifies session authenticity by collecting unique features from a device or browser and allows a positive identification during subsequent visits. Sigma Device can be utilized on a standalone basis and as an integrated part of a **Socure's** broader fraud solutions.

Socure KYC solution supports customer growth while bolstering compliance through accurate risk identification. **Socure** delivers a multi-dimensional view of a customer through patented AI and ML technology that leverages automated data ingestion and cleansing from hundreds of data sources to arrive at a single best-matched entity. **Socure's** proprietary database of cross-industry customer feedback data contains more than eight billion records tied to over one billion known good and bad identities providing organizations with high assurance decisions. **Socure** delivers pass rates of up to 98% for mainstream populations, and up to 94% for hard-to-identify

Socure

populations such as Gen Z, millennial, credit-invisible, thin-file, and new-to-country, ensuring inclusive access for all.

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 Predictive DocV verifies a consumer's government-issued identity document against their facial biometrics in seconds to approve more good customers during onboarding. The consumer captures an image of their document as well as a selfie, which initiates **Socure's** real-time image quality checks, front-to-back data matching, passive liveness detection, and selfie-to-ID photo match.

The result is an authentication process that can complement or replace existing verification methods. For example, DocV can be applied as a step-up solution for the most risky consumer segments, as a fallback to the KYC process, or as a top-of-the-funnel solution when required, such as in gaming and crypto industries. DocV is often used as a replacement for KBA or manual document verification processes due to its speed and accuracy. It is also complementary to data pre-fill solutions, where document data is passed back to the client and used to pre-populate name, address, and date of birth fields.

The benefits of DocV extend from fraud prevention to consumer conversion to implementation ease. DocV helps users stop spoofing attacks with enhanced facial biometrics, complete with NIST PAD L2 liveness detection. The solution's image capture technology ensures that +80% of users succeed in the capture process on the first attempt, often resulting in improved consumer conversion. Lastly, the lightweight SDK integration (both native and web based) as well as the no code customizable branding and workflows, offer expedited implementation timelines

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 that establishes trust between accounts and supports regulatory compliance.

Socure

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 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.

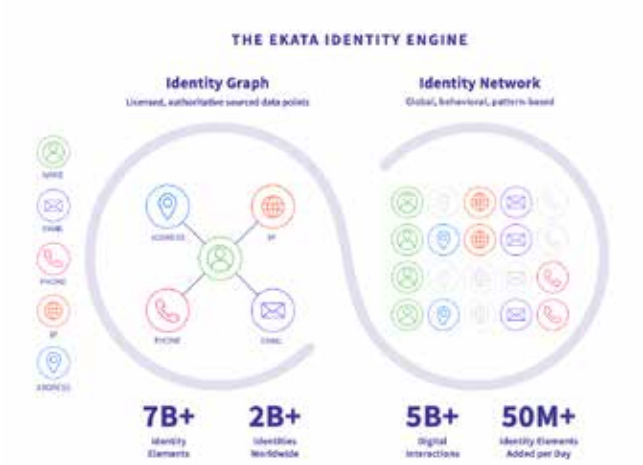
Ekata by Mastercard

Seattle-based **Ekata, a Mastercard company**, supports businesses in their effort to enable frictionless digital interactions and combat fraud worldwide with global identity verification data and risk insights.

Using the solutions, organizations can unify the elements of digital identities such as name, email, phone, IP address, and physical address—creating a 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 their solutions—converting billions of data elements into unique and valuable insights that allow businesses of all sizes to make accurate risk decisions about their customers.

The Identity Engine comprises two distinct and mutually exclusive data sources. Using these two data assets, **Ekata** applies data science and machine learning to produce solutions that integrate into businesses' decision platform, rules engine, and models.

- **Identity Graph:** Third-party sourced database that validates the five 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 by Mastercard

At a Glance:

- 3rd Party API Capabilities
- Machine Learning
- Pre-Authorization Functionality

Ekata by Mastercard

Ekata digital identity verification data seeks to build trust by solving two challenges:

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

With over 20 years of data sourcing experience and a global presence, **Ekata** helps over 2,000 companies verify that consumers are who they say they are, while fighting fraud in industries including ecommerce, financial services, and marketplaces.

Data Excellence

Ekata's credo is that "No single merchant or financial institution can collect adequate information to verify global digital identities involved in cross border transactions. Achieving data excellence is a competitive advantage in today's global identity verification and risk market."

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

- **Data sourcing practice:** The process to identify high quality, authoritative data providers across the globe.
- **Data Cleansing: Ekata** does a massive amount of data analytics and big-data engineering to clean, validate, and normalize the data for efficient use in fraud-prevention models.
- **Cross-border:** The solutions offer identity verification regardless of where organizations run their business (with the exception of embargoed countries).
- **Global:** With a global data approach, **Ekata** can cater to fraud problems globally. This focus allows clients to work with one provider for their identity verification needs regardless of their footprint.
- **Real-Time: Ekata** has put a lot of effort into building sophisticated real-time features. These features allow for the calculating and assessing of risk every 30 seconds. Additionally, transactions are standardized, normalized, and de-duplicated in 30 seconds to prevent counting duplicates or manual agent refreshes as new transactions.

Ekata also builds attributes which cannot be found elsewhere. This is because they are derived through some combination of **Ekata's** unique core IP assets. The solutions offer three types of derived attributes:

- **Data derived:** Confirms whether the identity used in a transaction is fake or real (does the email match the name?), confirms whether the identity is valid or not (is this email address valid?), and includes a second layer of intelligence

to confirm whether the identity is valid (how long ago was this email address created?).

- **Network derived:** A combination of global training data, data science and machine learning to produce three fraud models: IP Risk, Identity Risk Score, Network Score.
- **Model derived:** There are eight patterns across the data that identity network observes

Security and Privacy First

To **Ekata and its parent company Mastercard**, maintaining the privacy and security of personal data is paramount. To ensure the privacy of customers and data subjects, the Ekata Identity Network operates on pseudonymized data and probabilistic identity models. With billions of data points provided by customers, **Ekata's** proprietary Network provides the benefit of reducing privacy, regulatory, and security risks.

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

Ekata prioritizes respecting the individual rights of data subjects. We provide identity verification and fraud prevention services worldwide (except in embargoed countries), and have implemented a privacy and data protection program overseen by a global team of dedicated privacy, data protection, and security professionals. This team is responsible for ensuring compliance with legal and contractual privacy requirements set by global data privacy laws such as GDPR and CCPA. For more information about our privacy and data protection program, please explore our Privacy Overview at https://ekata.com/security-and-privacy/#Privacy. .

Ekata by Mastercard

Products

Identity verification suite

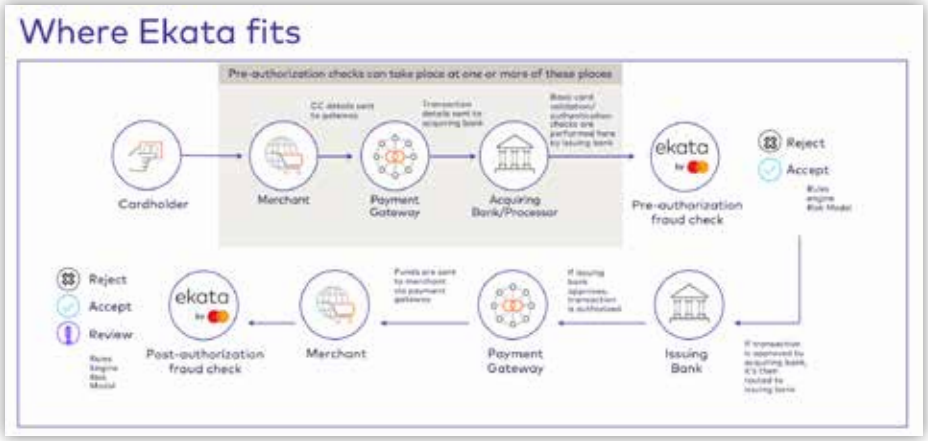
Automation:

Transaction Risk API

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

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

- **Validity checks** for payment details such as primary and secondary email, phone, and address provided by the customer
- **Match statuses** to confirm that the primary and secondary email, phone, and addresses provided in the transaction are associated with the customer
- **IP distance from address** calculations to gauge the distance between a provided IP and address
- **Risk flags and scores** to assess the risk of the holistic digital identity (Identity Risk Score), previous usage of identity elements (Identity Network Score), and the risk of a provided IP (IP Risk Flag)
- **Enriched phone metadata** to gain insight into the line type of the phone number



Account Opening API

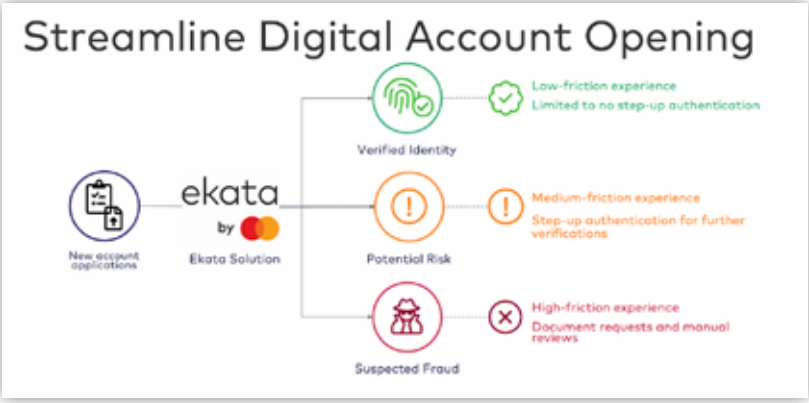
The Account Opening API identifies potential bad actors from good customers during the online application process. It is designed to expedite the user experience for good customers while preventing bad actors from using stolen or synthetic identities to gain instant credit, seek loans, launder money, or carry out credit bust-out schemes.

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

Ekata by Mastercard

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

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



Manual Review:

Pro Insight

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

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

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

Ekata by Mastercard

Identity element risk suite

Address Risk API

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

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

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

Phone Intelligence API

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

The Phone Intelligence API provides intelligence for risk analysis using:

- **Carrier information** to identify the company that provides voices and/or data services
- **Validity check** of a phone number
- **Country details** with access to the country calling code, country code, and country name associated
- **Prepaid account check** to understand whether the phone number is associated with a prepaid account
- **Unique identifier** that can be used to perform velocity calculations

Ekata by Mastercard

Integrations and Additional Services Offered

Pro Insight Integrations

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

API Integrations

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

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.

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.

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.

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.

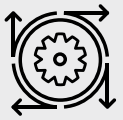
Onfido

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

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

Accertify Chargeback Services:

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

figure 1: user interface

Accertify
AN AMERICAN EXPRESS COMPANY

At a Glance:

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

Accertify Chargeback Services

Accertify's Chargeback Management solution can reduce the resources required to manage and respond to chargebacks by incorporating full or partial automation into the process. It offers a software-as-a-service platform that clients can manage themselves or they can outsource the end-to-end management of chargebacks using **Accertify's** 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 with the ability to create client-specific workflows based upon dollar values, chargeback reason, due date, client business needs, and other similar data points.

New additional integration: This 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:

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

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

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

Accertify Chargeback Services

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.

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

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

In 2023, Accertify's Roadmap will focus on a few key themes, including:

- Continuing to expand acquirer/processor global footprint
- Incorporation of new scheme policies such as the recent Visa First Party Misuse announcement
- Expanding and enhancing reporting capabilities and dashboards
- Developing a full end-to-end product for airlines and OTAs
- Continuing to enhance the user interface with a focus on improving client experience
- Expanding full representment automation capabilities

Sift Dispute Management

Sift is a leader in digital trust and safety, empowering businesses to unlock new revenue without risk. Sift dynamically prevents fraud and abuse with real-time machine learning (ML), a global data network of 70 billion events per month, and a commitment to long-term customer partnerships. Global brands such as DoorDash, Twitter, and Wayfair trust **Sift** to lower chargeback rates, proactively prevent online fraud, and fuel business growth.

Sift Dispute Management

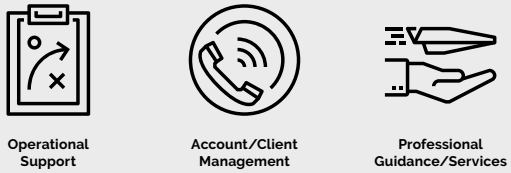
Sift Dispute Management is a chargeback management solution that helps businesses fight friendly fraud and win more disputes while simplifying the customer experience. **Sift** has added chargeback management to its Digital Trust & Safety Suite to help merchants stop invalid disputes, automate evidence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

Solutions & Functionality

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

The data that becomes compelling evidence varies, but typically includes a combination of payment processors, gateways, CRM, transactions, and orders. Bank issuers and card

At a Glance:

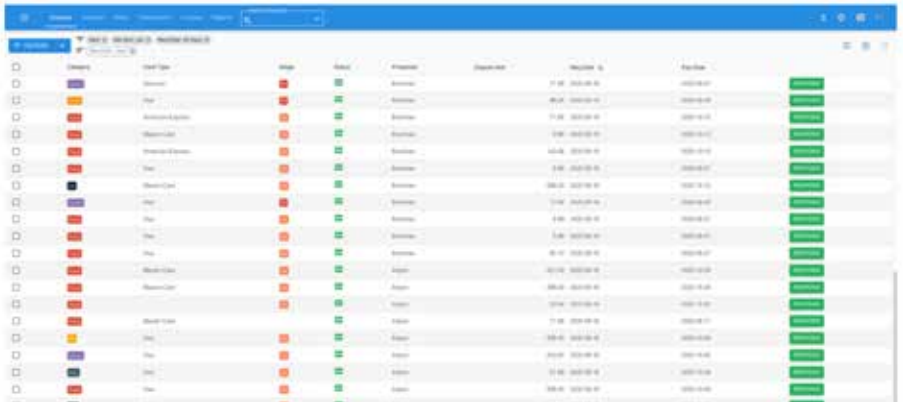


Sift Dispute Management

networks can also require additional evidence such as screenshots of delivered products. By aggregating the details from each source, the **Sift** Dispute Management Console allows merchants to take quick actions, for example, canceling and refunding orders, and creating dispute responses. The Console provides guidance and support at each stage of the dispute lifecycle to support maximum recovery of lost revenue.

Sift 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 Dispute Management

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

Once complete, the dispute responses are created and submitted automatically from the Console, with the option to auto-send them to the card network or to the issuer's required end-point. Response templates are now available that are customized to each decision makers' (card networks, issuing banks) requirements.

Through the Console, merchants benefit from the **Inquiries** tool. This functionality allows merchants to provide customer, order, and product details to the card brand dispute management platform—Order Insight® (Visa), and Consumer Clarity™ (Mastercard). This supplemental information is combined with the related card brand transaction data and made available to the dispute analyst at the cardholder's issuing bank.

With this enhanced level of detail, the dispute analyst is equipped to make better decisions on whether to allow the cardholder to file a dispute claim and if so, to more accurately choose what type of dispute should be filed. Typically, this level of customer detail, order detail, and product detail is not made available until well into the dispute process, and it can be accompanied by a message that a credit has been issued. This can also allow organizations to deflect many friendly fraud disputes, as well as chargeback fraud disputes that will be difficult to win.

Sift Dispute Management

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

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

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

Integrations

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

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

Services Offered

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

Sift Dispute Management

A team of Trust and Safety Architects, all of whom are industry experts with years of in-house fraud prevention experience, are available for consultation to help teams of all sizes establish and maintain a Digital Trust & Safety strategy. Support engineers are also available to answer any questions about product usage and technical details. Integration, account management, regular support, and assessments are all included. Premium support plans can be purchased based on volume and need.

In development in the next 6-12 months:

- New data processing system that allows **Sift** to support more volume, at higher speed
- Addition of alternate evidence that makes creating winnable responses even easier
- Connector refresh to simplify integration and easier data ingestion

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

Primary differentiators include:

- A hands-on, collaborative approach
- A method of becoming an extension of the client's fraud and loss prevention team
- Operating on both sides of the ecommerce transaction—on the front-end with order screening and on the back end with chargeback management support

ChargebackOps specializes in low-risk, ecommerce markets. This is due in large part to the requirement of customized responses, which most brands demand for their customers. When considering the lifetime value of a customer for an organization, the last thing they want is to increase friction for a customer who has been shopping with them for 10 years.

chargebackops
a ClearSale company

At a Glance:

Operational Support

Account/Client Management

Professional Guidance/Services

ChargebackOps

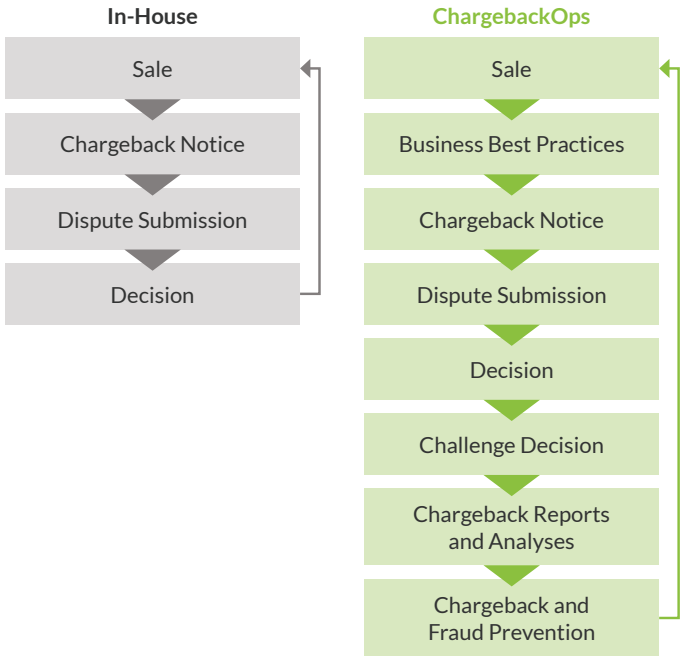
Keep authentic shoppers and build long-term customers.

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

As discussed above, the company's primary vertical is online ecommerce. Most clients also have physical storefronts for which chargebacks are processed, as well. Generally, **ChargebackOps** is willing to process chargebacks for any company who genuinely cares about their customers. During the sales process, they conduct a discovery about their industry, customer handling, and approach to dealing with chargebacks.

ChargebackOps offers two primary services:

- **Chargeback Management Service: ChargebackOps** offers a uniquely designed dispute resolution service for Fortune-500 ecommerce companies who prioritize the lifetime value of their customer and their brand. Using a hands-on and collaborative approach, their analysts investigate and respond to each



chargeback case in order to optimize the client's desired handling for all types of fraud.

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

- **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.

With order screening and chargeback management service, they operate on both sides of the ecommerce transaction. When using these services together, ChargebackOps offers clients a unique fraud viewpoint, measuring and scoring both order screening quality and opportunities to further develop fraud rules. With screening analysts dedicated to each client, they can score and treat each order in a customized fashion, providing customer service experiences similar to that of a client's own employees.

Rules development and management support are provided. However, ChargebackOps aims to empower clients to manage their own rule management process. Significant data, close collaboration, conversations, filters, and rule recommendations are provided on a regular basis. Additional ad-hoc feedback is provided by agents who review chargebacks, identifying and relaying fraud trends back to merchant clients. This feedback loop is a true differentiator of ChargebackOps.

Three types of reporting are currently available, all included in the price of the service.

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

or can be emailed automatically.

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

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

Proof-of-concept process:

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

Pricing

Chargeback Management

While they offer a variety of pricing models, the most common approach includes fixed-monthly billing. In order to establish the fixed-monthly price, a client's past 12-months of chargebacks are reviewed and a customized quote is provided. In addition to fixed-monthly billing, a tiered structure and a hybrid recovery model/ tiered structure exist as well as a 100% recovery model depending on the client.

ChargebackOps

Order Screening & Review

The most common pricing model includes per-review structuring, using a Fill-A-Tier model which works by extending discount tiers once the previous tier has been met. Pricing generally begins with a ceiling of $4 per review and a floor of $3 per review.

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

Integration

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

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

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.

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.

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:

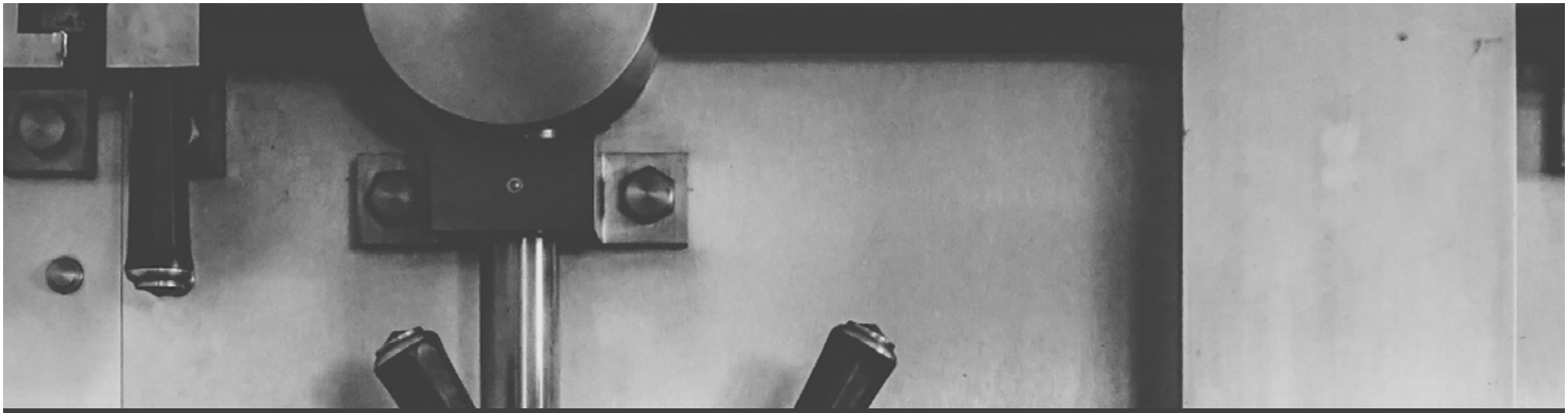
- **Eliminate Chargebacks:** They stop and prevent chargebacks before they happen. They combine a **Cardholder Dispute Resolution Network** and **Order Insight**, a patent-pending platform that connects cardholders, merchants, and issuers to resolve billing confusion and disputes in real-time. This essentially 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.