KUPPINGERCOLE ANALYSTS

Fraud Reduction Intelligence Platforms - Finance

John Tolbert

June 23, 2025

This report provides an overview of the Fraud Reduction Intelligence Platforms (FRIP) market for finance, banking, and payment services, as well as a compass to help you find a solution that best meets your needs. It examines solutions that provide an integrated set of security and compliance capabilities designed to protect financial, banking, and payment applications. It provides an assessment of the capabilities of these solutions to meet the needs of all organizations to monitor, assess, and reduce these risks.

Executive Summary

Fraud remains a significant and evolving threat to businesses, non-profit organizations, and government agencies worldwide. While banking, finance, payment services, and retail remain primary targets, other sectors including insurance, gaming, telecommunications, healthcare, cryptocurrency exchanges, government assistance agencies, travel and hospitality, and real estate are increasingly vulnerable. Cybercriminals continually refine their Tactics, Techniques, and Procedures (TTPs) to exploit gaps in security controls, identity proofing, and transaction verification. Banks, other financial institutions, merchants, and payment service providers must use sophisticated fraud detection systems to prevent fraud of various types. Businesses across the world of all sizes and across most industries are negatively affected by fraud. Non-profit organizations and government agencies are also increasingly targeted. All organizations are at risk of loss from the many different kinds of fraud perpetrated today.

As fraud tactics evolve, organizations must continually adapt their detection and prevention frameworks, leveraging Machine Learning (ML)-driven fraud intelligence, real-time transaction analysis, and identity verification enhancements to mitigate financial and reputational risks.

A major fraud mitigation strategy is to use a FRIP which enhances fraud detection through six main components: identity verification, credential intelligence, device intelligence, user behavioral analytics, behavioral/passive biometrics, and bot detection.

This report focuses on FRIP solutions that can help organizations in the financial sector. The types of fraud experienced and use cases are somewhat different from those in other sectors, although there are significant overlaps. Moreover, while all six major functional areas of FRIP solutions can be used by banks, fintechs, and other financial institutions, regulations mandating Anti-Money Laundering (AML), Know Your Customer (KYC), and sanctions screening require financial organizations to have more rigorous Identity Verification (IDV) solutions. Sanctions screening includes checking updated lists such as the US Office of Foreign Asset Control (OFAC), United Nations (UN) sanctions list, European Union () consolidated list, UK consolidated list, and others. These enhanced IDV and screening measures need to be undertaken during onboarding, in regular periodic checks (defined by regulations), and sometimes during transactions. Screening actions apply to named individuals and organizations as well as financial accounts. Failure to screen effectively can result in significant legal, financial, and reputational consequences, including regulatory fines and sanctions of the screening entity itself.

For information about the Leadership Compass process, see our KuppingerCole Leadership Compass Methodology.

Types of Fraud

Account Takeover (ATO) Fraud

ATO fraud occurs when fraudsters gain unauthorized access to a legitimate user's account to conduct illicit activities. Attack vectors include:

- Credential stuffing and password spraying using breached credentials.
- Malware-based attacks (for example, Man-in-the-Middle [MitM] or Man-in-the-Browser [MitB]).
- Social engineering scams leveraging phishing, smishing (SMS phishing), and vishing (voice phishing).
- Remote Access Trojans (RATs) that enable fraudsters to control compromised devices.
- Rootkits and info-stealer malware that give unauthorized access to PII and user credentials to fraudsters.
- SIM swap fraud, in which attackers transfer a victim's phone number to a new SIM to intercept OTPs and reset account access.
- Session hijacking, where fraudsters either use MitM tactics or purchase long-lived valid sessions on the dark web.

Account Opening (AO) Fraud / New Account Fraud (NAF)

AO fraud and NAF are terms often used interchangeably, and both forms involve the use of stolen personal data to create fraudulent accounts. NAF may also include synthetic fraud (see below). Fraudsters may exploit breaches of Personally Identifiable Information (PII) from financial, healthcare, educational, and government sources to fabricate a complete digital identity. These fake accounts are commonly used to:

- Access credit lines, loans, and instant financing.
- Conduct promotion abuse.
- Funnel money through mule accounts to facilitate money laundering.
- Commit Buy-Now-Pay-Later (BNPL) and small business loan fraud.

Synthetic Identity Fraud

Distinct from AO fraud but part of NAF, synthetic identity fraud involves the creation of entirely new digital personas by combining real and fictitious identity attributes. Rather than exploiting a single stolen identity, fraudsters generate synthetic profiles by:

- Assembling non-existent or mismatched Social Security Numbers (SSNs) or other official ID types with real addresses and phone numbers.
- Exploiting gaps in identity verification processes.
- Gradually building a credit profile through small transactions and loans before executing larger-scale fraud (a technique known as "busting out"). Synthetic identities are harder to detect because they do not correspond to real individuals who would report fraudulent activity.

Emerging Fraud Trends and Scams

Fraud tactics continue to diversify across digital channels. Categories include:

Digital Impersonation Scams:

- Fake investment platforms (cryptocurrency, gold, foreign currency exchange, and real estate scams).
- Deepfake audio/video used in corporate payment scams, customer account enrollment attacks for AO/NAF.
- Artificial Intelligence (AI)-assisted social engineering for crypto and romance scams and Business Email Compromise (BEC).
- CEO/CFO fraud involving payment redirection.
- Fake job listings designed to harvest PII and banking details.
- Fake government, welfare, and tax refund notices designed to steal personal information.

Payment and Financial Fraud:

- Card-Not-Present (CNP), Card-Not-Received (CNR), counterfeit card, and skimmer fraud.
- Malicious invoice payment redirection targeting businesses.
- Fraudulent real estate escrow redirection using compromised email accounts.
- Unauthorized BNPL transactions exploiting weak identity verification.
- Authorized Push Payment (APP) fraud where victims initiate transactions at the behest of fraudsters, often in cases of crypto, romance, invoicing, or purchase scams.

Automated and Bot-Driven Fraud:

- Automated credential stuffing and brute force attacks.
- Inventory hoarding (Grinch bots) that disrupt retail stock availability.
- Fake account creation bots that execute promotional abuse.
- Gift card cracking, where bots guess activation codes for financial gain.
- Fake reviews, social media manipulation, and ad fraud bots.

Cryptocurrency Fraud:

- Fake Initial Coin Offerings (ICOs) designed to defraud investors.
- Wallet-draining malware and clipboard hijacking of crypto addresses.
- Fraudulent exchanges and aggregators tricking users into depositing funds.

Fraud Mitigation Strategies

Organizations combat fraud through layered security approaches that leverage:

- FRIPs: Enhancing fraud detection through six key components:

  - Identity verification.
  - Credential intelligence for compromised account detection.
  - Device intelligence to track devices previously used for fraud and to aid in discovery of anomalous behavior.
  - User behavioral analytics to assess deviations from normal activity.
  - Behavioral/passive biometrics to identify individual users via their normal interactions with their devices, discover coercion, and flag fraudulent interactions.
  - Bot detection and mitigation to prevent large-scale automated fraud.

- Real-time risk analytics: Assessing transaction and behavioral anomalies from sources described above to provide decisions, risk scores, and context for customer applications. Not every FRIP solution contains all six primary sets of functionality, and even those that do commonly have integrations with external services. Orchestration of both internal and external capabilities is often needed for fully integrated FRIP solutions.
- Risk-based Authentication (RBA) within Customer Identity and Access Management (CIAM) systems: Strengthening identity verification by considering credential intelligence, device reputation, and behavioral biometrics, often in conjunction with FRIPs.

Key Findings

As fraudsters change their TTPs and find new nefarious ways to exploit victims, FRIP solution providers continue to innovate to help their customers deter fraud.

Identity verification is paramount, not only at account opening time, but also periodically. Some solutions are moving toward continual IDV.
FRIP solutions today need to have at least basic AML, KYC, Politically Exposed Persons (PEPs), and sanctions screening capabilities, either built-in or available via third-party services. However, many vendors are lagging in this area.

- AI-powered photo, audio, and video deepfakes are a growing problem, and some solutions are addressing these vectors.

Generative AI (GenAI) is helping scammers create more convincing phishing emails.

- Scams like those described above (investment, crypto, romance, impersonation, etc.) are now the most common types of fraud encountered, even outpacing ATOs.
- Info-stealer malware has risen in popularity amongst fraudsters, which helps them get valid credentials and PII for ATO and NAF.
- Viral social media “challenges” have encouraged users to commit financial crimes.
- SMS phishing (smishing) attacks, for example with messages purporting to be from toll payment services and delivery services, are on the rise.
- FRIP solutions are enhancing detection capabilities with ML and Deep Learning (DL).

Leading-edge FRIP solutions are adding gGenAI capabilities to their investigative interfaces to assist fraud analysts in their investigations and to provide reports.

Market Analysis

The market for FRIPs is growing proportionally with the rise in frequency and complexity of fraud itself.

The FRIP market is somewhat active in terms of mergers and acquisitions. In October 2024, Experian agreed to acquire ClearSale in Brazil, adding significant market share in a large market.

In April 2024, Entrust completed its acquisition of Onfido, a prominent identity verification company specializing in AI-driven solutions.

LexisNexis® Risk Solutions acquired IDVerse® in 2024 and will integrate IDVerse's document authentication and biometric verification into its Dynamic Decision Platform.

In this edition of the Leadership Compass on FRIP for Finance, we have new vendors participating that have not been in previous versions, including Entersekt, Futurae, LynxTech, Sumsub, Tietoevry, and XTN Cognitive. We expect further growth in the FRIP market. Delivery Models

Most FRIP services are offered as Software as a Service (SaaS), with customer applications calling the protected Application Programming Interfaces (APIs) of the FRIP solutions. Some vendors offer software that customers can run on-premises or in private clouds.

IDV components are a combination of built-in services, apps, Software Development Kits (SDKs), and APIs. IDV apps are typically mobile apps that can take photos of authoritative government IDs or documents and selfies (for photo matching) and use Near Field Communication (NFC) to scan embedded chips. Some vendors lean heavily on third-party services for IDV functions.

The device intelligence and behavioral biometrics components are most commonly implemented as JavaScript. The .js files run in the browsers and apps of the customers' customers, harvesting many attributes for analysis. Alternatively, some vendors provide SDKs that can pull similar information for their customers to use to build apps and sites.

Compromised credential intelligence, if performed only in-network, only uses data about failed and suspicious logins and transactions from within the FRIP solution provider's ecosystem of customers. A few vendors expand their capabilities by pulling risk signals from external sources such as haveibeenpwned, VeriClouds (acquired by Enzoic), and SpyCloud.

User Behavioral Analysis and bot detection and management capabilities, if present, are hosted by the FRIP (unless customers choose to run it themselves). User Behavior Analytics (UBA) depends on identity and transaction data, and bot detection is most effectively implemented via behavioral biometrics, and augmented by rules, Cyber Threat Intelligence (CTI), and ML detection algorithms.

Required Capabilities

This Leadership Compass analyzes FRIP solutions for financial organizations that help reduce the following types of fraud and financial crime:

- ATO
- AO, synthetic identity, and NAF
- Payment transaction fraud
- Credit card issuer fraud
- Scams targeting businesses and individuals
- Money laundering and sanctions violations

The following are key capabilities that FRIP solutions for financial organizations need:

Solution Basics

- Well-documented APIs for customer app integration
- API management and security
- JavaScript and SDKs for client telemetry harvesting
- Multifactor Authentication (MFA) and Role-Based Access Controls (RBAC) for administrators
- Toolkits for customizing connectors
- Auditing, reporting and dashboarding
- Scalable service architecture & high-availability deployment
- Use of ML and Deep Learning (DL) algorithms for risk analysis
- Integration with customer Information Technology Service Management (ITSM)
- ISO 27001 and SOC 2 Type 2 certification
- Features for 3DS2.x compliance
- Features to support compliance with the second and third Payment Service Directives (PSD2/3) from the European Union (EU)

Payment and Financial Fraud Reduction

- Detection and prevention of CNP fraud
- Detection and prevention of APP and BNPL fraud
- Detection and prevention of mule account onboarding and transactions
- Detection and prevention of payment misdirection
- Detection and prevention of scams

Identity Verification

- Built-in user attribute verification
- Integration with third-party identity verification and authoritative attribute providers
- Facilitation of AML, KYC, and name/watchlist screening
- APIs and SDK for identity verification application development

Credential Intelligence

- Use of credential intelligence from within the vendor’s network of customers

- Inclusion of credential intelligence from external Identity Providers or third-party sources

Device Intelligence

- IP reputation
- Geo-location & geo-velocity detection
- Mobile network and Wi-Fi network analysis
- Device ID, type, and fingerprint
- Device reputation
- Device posture checks, including OS version and malware detection
- SIM swap detection
- Known user on unknown device checking
- Device jailbreak/rooted checking

User Behavioral Analysis

- Login context analysis, including frequency and time of logins, and login locations
- Transaction details and historical analysis, transaction types, amounts, item analysis, velocities and frequencies, locations, proximity to suspicious behavior such as phishing, relationships to known high-risk accounts, account creation clusters, and more
- Data privacy compliance, including the use of privacy-enhancing technologies such as de-identification, pseudonymization, redaction, encryption, and others

Behavioral Biometrics

- Obfuscated JavaScript and secure SDK implementation
- Wide range of features and modalities which can be examined from computers and mobile devices

Bot Detection & Management

- Ability to detect bot vs. human users
- Ability to identify bot intentions (good, gray, or malicious)
- Ability to deploy unobtrusive or user-friendly challenges
- Policy-based bot handling, including redirection and throttling

Risk Engine

- Customizable orchestration of internal components and third-party services
- Customer configurable risk policy authoring
- Risk score and/or decisions output
- Score rationale output
- Integration with third-party authentication services
- Integration with CIAM systems
- Integration with customer Line of Business (LOB) applications

Innovative Capabilities (Selection)

- Credential and device intelligence signals sharing
- Biometrics and liveness detection for remote identity verification and authentication apps
- Deepfake detection
- Detection of CNR, counterfeit card usage, and skimmers
- Detection of complex scams, such as crypto and romance scams
- Emphasis on unobtrusive methods for fraud detection
- Use of GenAI in the fraud analyst interface, including Natural Language (NL) queries, case descriptions, and executive reporting
- No-code/low-code policy authoring interface
- Map, timeline, and identity/transaction graph views for fraud analysts
- Attribute-Based Access Controls (ABAC) and/or Policy-Based Access Controls (PBAC) for administrators
- Integration with call centers
- Integration with customer Security Information and Event Management systems (SIEM)
- Support for detecting sophisticated smishing, vishing, and quishing
- Facilitation of the filing of Suspicious Activity Reports (SARs)
- Payment Card Industry Data Security Standard (PCI DSS) certification
- Take-down services

Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identify vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept (PoC) of pilot phase, based on the specific criteria of the customer.

Based on our rating, we created various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for:

- Product Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership

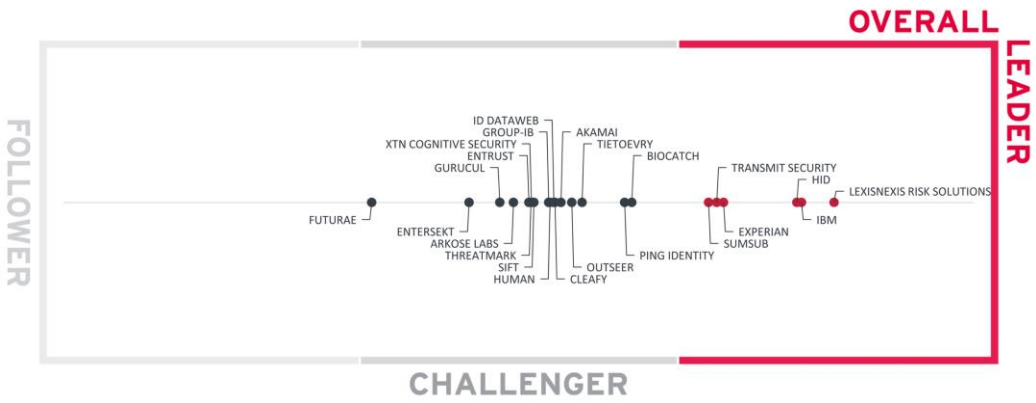


Figure 1: Overall Leadership in the FRIP for Finance market

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right. The rating provides a consolidated view of all-around functionality, market presence, and financial security.

However, these vendors may differ significantly from each other in terms of product features, innovation, and market leadership. Therefore, we recommend considering our other leadership categories in the sections covering each vendor and their products to get a comprehensive understanding of the players in this market and which of your use cases they support best.

LexisNexis Risk Solutions, HID, and IBM are clustered at the top of the Overall Leaders Chart. All three vendors provide extensive FRIP capabilities, leading-edge innovation, and significant market share. LexisNexis Risk Solutions has assembled a complete FRIP solution, based upon their own products and wise acquisition strategy. HID is a leading high-assurance identity provider enabled by Identity and Access Management (IAM) technologies

utilizing HID's trusted identity ecosystem, including hardware and software products that prevent fraud. IBM's Trusteer can also be tightly integrated with not only their Security Verify products but also many other business applications. Experian, Transmit Security, and Sumsub are also Overall Leaders in this edition, and each have excellent products and commanding market positions. Experian is well-known as a credit rating agency and thus has deep insights into consumer accounts. Transmit Security is highly innovative and integrates FRIP with its CIAM platform. Sumsub is an anti-fraud specialist debuting as a Leader in this report.

The majority of the vendors appear in the Challengers section. Since this report focuses on FRIP for the finance industry, there are some new companies in this report that were not in previous versions. Because of the focus on financial use cases, the positioning of vendors and products is somewhat different than earlier Leadership Compasses on FRIP.

There are no Followers in this overall leadership rating.

Overall Leaders are (in alphabetical order):

- Experian
- HID
- IBM
- LexisNexis Risk Solutions
- Sumsub
- Transmit Security

Product Leadership

Product leadership is the first specific category examined below. This view is mainly based on the presence and completeness of required features as defined in the required capabilities section above. The vertical axis shows the product strength plotted against the combined/overall strength on the horizontal axis. The Product Leadership chart is rectangular and divided into thirds. Product Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

Figure 2: Product Leadership in the FRIP for Finance market

IBM, HID, Transmit Security, LexisNexis Risk Solutions, Experian, and Sumsub are the top Product Leaders. Given the focus on finance, product leaders must have good IDV capabilities, transactional risk analysis, account opening/new account/synthetic identity fraud detection, APP fraud and scam detection, support for AML and KYC, name/watchlist

screening, and orchestration, among other features. The Product Leaders here have the most complete mix of those features.

The bulk of the vendors appear in the Challengers section, and only one vendor placed as a Follower. Many excel in multiple areas of the required capabilities but may be missing one or more essential functions. Since many banks, fintechs, issuers, and payment processors utilize several fraud detection and prevention components, organizations that are looking for such components must consider the individual strengths and challenges of all the vendors surveyed here. A more detailed analysis follows in the Product/Vendor Evaluation section.

Product Leaders (in alphabetical order):

- Experian
- HID
- IBM
- LexisNexis Risk Solutions
- Sumsub
- Transmit Security

Innovation Leadership

Next, we examine innovation in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

This view is mainly based on the evaluation of innovative features, services, and/or technical approaches as discovered in the course of our research. The vertical axis shows the degree of innovation plotted against the combined/overall strength on the horizontal axis. The Innovation Leadership Chart is rectangular and divided into thirds. Innovation Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

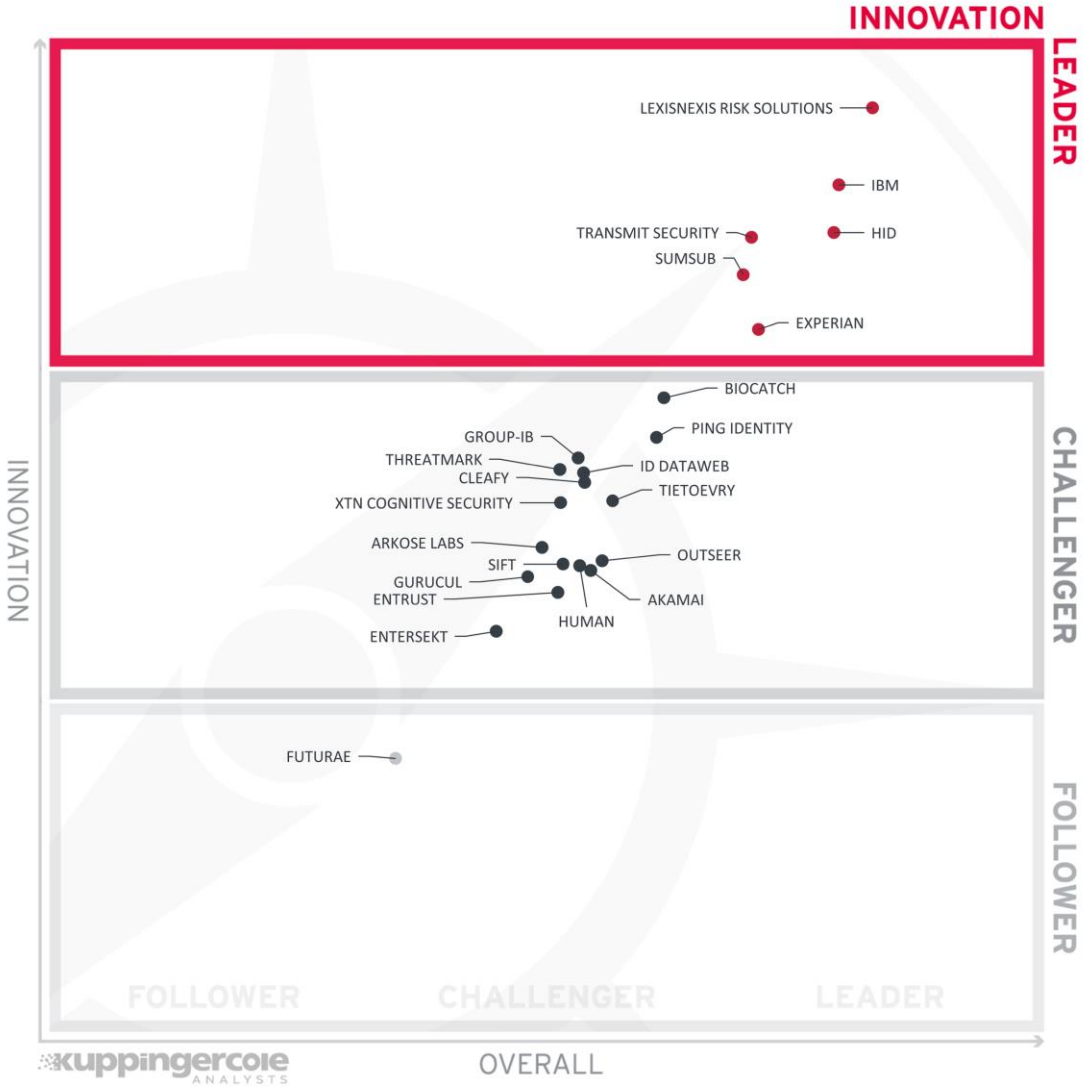


Figure 3: Innovation Leadership in the FRIP for Finance market

Innovation Leaders are those vendors that are delivering cutting-edge products, not only in response to customers' requests but also because they are driving the technical changes in the market by anticipating what will be needed in the months and years ahead. There is a correlation between the Overall, Product, and Innovation Leaders, which demonstrates that leadership requires feature-rich products that are looking over the horizon to bring advancements to help their customers.

The Innovation Leaders are LexisNexis Risk Solutions, IBM, HID, Transmit Security, Sumsub, and Experian. Most vendors appear in the Challenger area, with only one in the Follower section. It is important to note that Challengers and Followers also usually have one or more innovative features, and each should be considered when looking for FRIP solutions.

Innovative features in FRIP for finance include apps/SDKs for remote onboarding with liveness detection and deepfake detection; use of GenAI for queries, case descriptions, and reports; advanced orchestration for onboarding and investigation workflows; intuitive analyst UIs that include drill-down, timeline and map views, and identity/transaction graphs; detailed support for AML/KYC including enhanced due diligence; scam intervention techniques; use of ML and DL for device intelligence, UBA, and behavioral biometrics; implementation of unusual modalities for behavioral biometrics; more extensive list of attributes considered for UBA; and more.

Innovation Leaders (in alphabetical order):

- Experian
- HID
- IBM
- LexisNexis Risk Solutions
- Sumsub
- Transmit Security

Market Leadership

Finally, we analyze Market Leadership. This is an amalgamation of the number of customers, the number of transactions evaluated, the ratio between customers and managed identities/devices, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and the financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

In this chart, the vertical axis shows the market strength plotted against the combined/overall strength on the horizontal axis. The Market Leadership Chart is rectangular and divided into thirds. Market Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

Figure 4: Market Leaders in the FRIP for Finance Market

Market Leaders in FRIP for finance include HID, Experian, LexisNexis Risk Solutions, Outseer, IBM, Entrust, and Akamai. These companies have substantially different backgrounds, ranging from credit rating, credential issuance and IAM, content delivery network, IT stack vendor, and a FRIP specialist.

The majority of the firms are Challengers in the FRIP for finance market. Many of them are FRIP specialists. Given the increasing amount of fraud and scams, there is room for growth for all these vendors.

Market Leaders (in alphabetical order):

- Akamai
- Entrust
- Experian
- HID
- IBM
- LexisNexis Risk Solutions
- Outseer

Product/Vendor evaluation

This section contains a quick rating for every product/service we have included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For this market segment, we look at the following categories:

IDV - This category rates the quantity, quality, and jurisdictional variety of integration and interoperability capabilities for identity verification as defined in Chapter 1. Many FRIP services programmatically query specialty third-party identity vetting services. ID Proofing is not merely performing transaction time comparisons to templates created at registration time. Rather, this metric considers built-in functions (including the presence of mobile apps and SDKs for remote onboarding, photo/face matching, and ID document verification), configurable callouts to authoritative attribute providers, and indirect support for AML/KYC. Liveness detection, of both documents and users, helps detect spoofed, deepfaked, or synthetic submissions. IDV is a primary means of reducing AO, NAF, and synthetic identity fraud and is a regulatory requirement in financial use cases in many jurisdictions.

Credential Intelligence – This category refers to information about prior usage of digital credentials, to answer questions such as “has this credential known to have been recently compromised?” or “has this credential been used for fraud at other sites?”. Some FRIP vendors aggregate credential intelligence from across their customer bases. Others receive and process such information from third-party services, although this is still uncommon.

UBA – This category assesses the capabilities with regard to processing historical information about the subject user and past transactions to determine baseline profiles for analysis against current request contexts to identify and classify anomalous behavior. Examples of common UBA parameters include frequency/time of logins, failed login patterns, transaction types and amounts, transaction frequency/velocities, transaction locations, payees, exceptions for known travel, transaction item analysis, transaction proximity to other suspicious activities (such as phishing or smishing), discernment of multiple transaction attempts from multiple users from a single device or IP, relationships to known high-risk accounts, and user profile changes. UBA is a key method for preventing ATO, credit card and other payment fraud, and scams.

Device Intel - This category is the combination of device intelligence parameters including device fingerprint, type, health assessments, device and IP reputation, etc., as described in Chapter 1. FRIP services commonly draw upon multiple sources, both internal and external. Some of the vendors examined below provide these functions to other FRIP vendors. Device

intelligence is a key method for preventing ATO fraud and a contributing element to preventing AO, credit card, and other payment fraud.

Behavioral Biometrics – This measures the presence and sophistication of behavioral biometrics within the solution. Behavioral biometrics is generally implemented as JavaScript downloaded to consumer browsers and information collected from mobile devices by vendors' SDKs. Behavioral biometrics can create profiles on users based on their interaction with keyboards, mice, and touchscreens as well as certain device specific parameters. Behavioral biometrics is a key method for preventing ATO fraud and a secondary means for preventing AO, payment fraud, and some types of scams.

Bot Detection - This category considers the ability of vendor solutions to analyze traffic in real-time to accurately identify whether it is initiated by legitimate users or bots. In many cases, bots are detected through behavioral biometrics, but some services utilize overt methods that require end user interaction, activity signatures, cyber threat intelligence, and manual analysis. Bot management addresses how the vendor services aid customers in handling bots. Common options are challenging, redirection, and throttling. Bot detection and management can help prevent automated ATO and AO fraud attempts. While bot detection is considered essential for finance use cases, certain aspects of advanced bot management are treated as innovative in this edition.

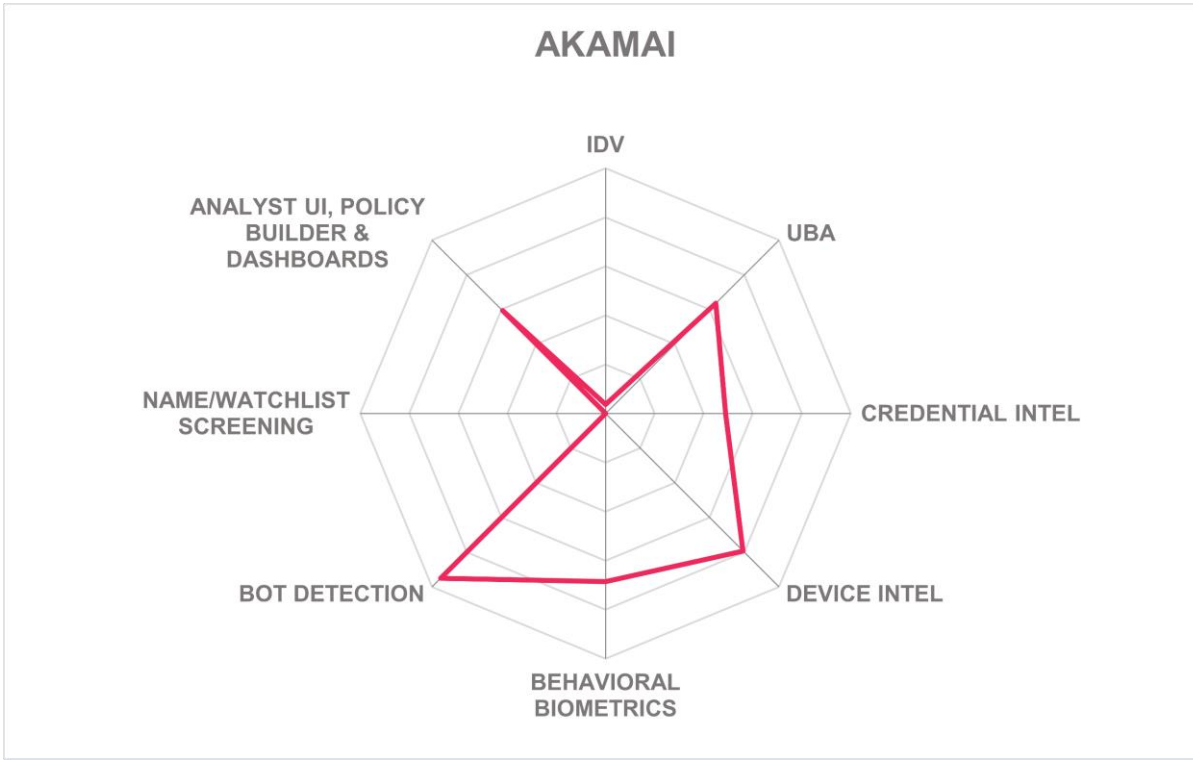
Name/Watchlist Screening – This category incorporates techniques and processes built-in to solutions and/or called via APIs that enable Anti-Money Laundering (AML), Know Your Customer (KYC), and name/watchlist/sanctions screening. AML processes focus on detecting and preventing the laundering of illicit funds by monitoring transactions, identifying suspicious activities, and ensuring regulatory reporting. KYC involves verifying customer identities, assessing risk profiles, and maintaining accurate records to confirm the legitimacy of individuals and entities. Sanctions screening checks customers and transactions against global sanctions lists to prevent dealings with prohibited individuals, organizations, or countries. Supporting technologies include automated identity verification platforms, risk scoring engines, and machine learning models that analyze large datasets to detect patterns indicative of fraud or financial crime. Real-time screening tools cross-reference data with updated sanctions, PEPs, and adverse media lists, while advanced solutions integrate with transaction monitoring systems and leverage AI to reduce false positives and enhance detection accuracy. AML, KYC, sanctions and PEP screening are important for financial crime compliance and Customer Due Diligence (CDD).

Analyst UI, Policy Builder & Dashboards – This metric considers solutions' management and analyst interfaces. Analyst UIs include case management, search features (which may be enhanced by GenAI), timeline/map/graph views, and the ability to drill down into details and pivot on attributes. Policy builders are generally of two types: a modern flowchart style into which authors can drag-and-drop elements and select attributes and name/value pairs; or an older, sequential list of conditions, selected via drop-down lists and connected with logical operators. The flowchart style is preferred due to its more intuitive nature. Moreover, the flowchart style makes it easier to orchestrate both internal and external services for maximum effectiveness. Dashboards should present the most pertinent info in an efficient way and allow customization per user. The Dashboard rubric also includes a measure of the

types of standard reports available, and the ability to customize reports as needed. This quality of this component is essential for facilitating investigations, providing succinct but useful information, and crafting risk evaluation policies.

Each of the product/service sections below follows a similar structure in order to make it easier for readers to compare features between vendors.

Akamai – Account Protector, Bot Manager, Brand Protector, Content Protector, Client-Side Protection & Compliance



Leader in

Akamai Technologies is a cloud and security provider headquartered in Cambridge, Massachusetts, in the US. Founded in 1998, the company is one of the veteran players in the market, providing a broad range of security, compute, and delivery solutions through its Akamai's globally distributed infrastructure, one of the world's largest distributed edge and cloud platforms. For FRIP, the Akamai offering is composed of the above listed services, which address the device intelligence, user behavioral analysis, behavioral biometrics, and bot detection and management components. The services are part of their Content Delivery Network (CDN) platform, rather than an API-driven SaaS, and are run from their own facilities and public Infrastructure as a Service (IaaS) providers across global datacenters. Android and iOS SDKs are available for customer app integration, and JavaScript is used for browser interactions. Costs are based on legitimate traffic volumes for web application security products with zero-overage fixed fees. There is a separate fee for SDK usage. Customer applications call Akamai services via the REST API, and JavaScript Object Notation (JSON) formats are supported.

Akamai does not support functions related to AML or KYC compliance, or name/watchlist screening. It does not facilitate SAR or provide support for the 3-D Secure 2 (3DS2) and PSD2 standards. However, Akamai has support for PCI DSS compliance with its Client-Side Protection & Compliance product, which helps mitigate data exfiltration threats to aid in compliance with PCI DSS v4.0 requirements through advanced script detection and real-time alerts. Akamai Account Protector helps with PCI DSS compliance for secure transaction protection. Akamai does not provide specific solutions for EMVCo 3DS 2 or EU PSD2 compliance.

Akamai's Account Protector helps to mitigate CNP fraud by monitoring abnormalities in user behavior during payment flows. The solution also detects malicious card testing attempts and provides some capabilities for screening for money mule account creation and BNPL fraud. Akamai offers extensive industry-specific support, notably in the travel/hospitality, retail, and insurance sectors, providing some protection against various types of scams, including crypto scams such as pig butchering.

Akamai does not have IDV services per se but can detect abnormal behavior and suspicious email addresses during registration. It can integrate with Ping Identity’s CIAM solution, but there are no other third-party IDV service connectors. The platform uses in-network credential intelligence only. This limits its ability to detect NAF and synthetic fraud. In terms of device intel, Akamai examines the basic parameters and can identify known users on new devices. The platform does not support jailbreak or malware detection or SIM swap detection directly. The UBA functions evaluate various attributes like login locations, failed login patterns, transaction velocities, and other indicators to discern suspicious activity and prevent ATOs. Data retention policies are compliant with global privacy regulations like GDPR, CCPA, and can be defined per customer. Akamai employs behavioral biometrics, instantiated as SDKs for Android, iOS, Cordova, Ionic, Flutter, React Native, and Xamarin, examining features such as keystroke, swipe, scrolling, gyroscopic, accelerometer, and app usage analysis. Their behavioral biometrics enable bot management capabilities, which also utilize embedded pixels for bot detection, allow distinctions between benign and malicious activities, and support configurable allow/denylists with throttling, redirection, and challenge-response mechanisms.

Their risk engine allows for graphical visualization and configuration of risk evaluation policies. The policy builder interface is intuitive, with sliders for adjusting the weight of risk factors. It can output risk scores with explanations for customer apps. The results from the risk engine can also be packaged as HTTP headers and JSON. Akamai supports Representational State Transfer (REST) APIs and webhooks for data exchange, but better API authentication methods should be supported. Akamai does not have ITSM connectors. Akamai's solutions do not currently offer integration with call center systems. Their fraud analytics interface includes customizable, widget-based dashboards for real-time monitoring and a variety of report types, including anomaly and fraud type detection, but it is not designed as a case management platform. Furthermore, the analyst interface employs GenAI to generate executive reports and summaries and supports NL queries.

Akamai is certified against ISO 27001/27017/27018, SOC 2 Type 2, AU IRAP, and UK Cyber Essentials. Akamai has obtained an Attestation of Compliance for PCI DSS 4.0. As a

multi-cloud native solution with edge datacenters across four continents, Akamai's FRIP services are highly scalable. Akamai offers training and support in many languages. Akamai relies on clients to manage consent for processing data attributes and assumes consent through customer relationships. The company employs privacy-enhancing technologies such as data anonymization, pseudonymization, aggregation, redaction, and encryption to secure data. Akamai has customers across various industries, such as insurance, healthcare, travel/hospitality, gaming, retail and eCommerce, media, electronic service providers, advertising, government agencies, telecommunications, and utilities. Its lack of IDV, case management, and ability to detect certain types of financial fraud mean that it would need to be deployed with other finance-focused FRIP solutions with integrated fraud analyst interfaces. Financial organizations that use Akamai CDN services and those that need advanced device intelligence and bot management should consider Akamai.

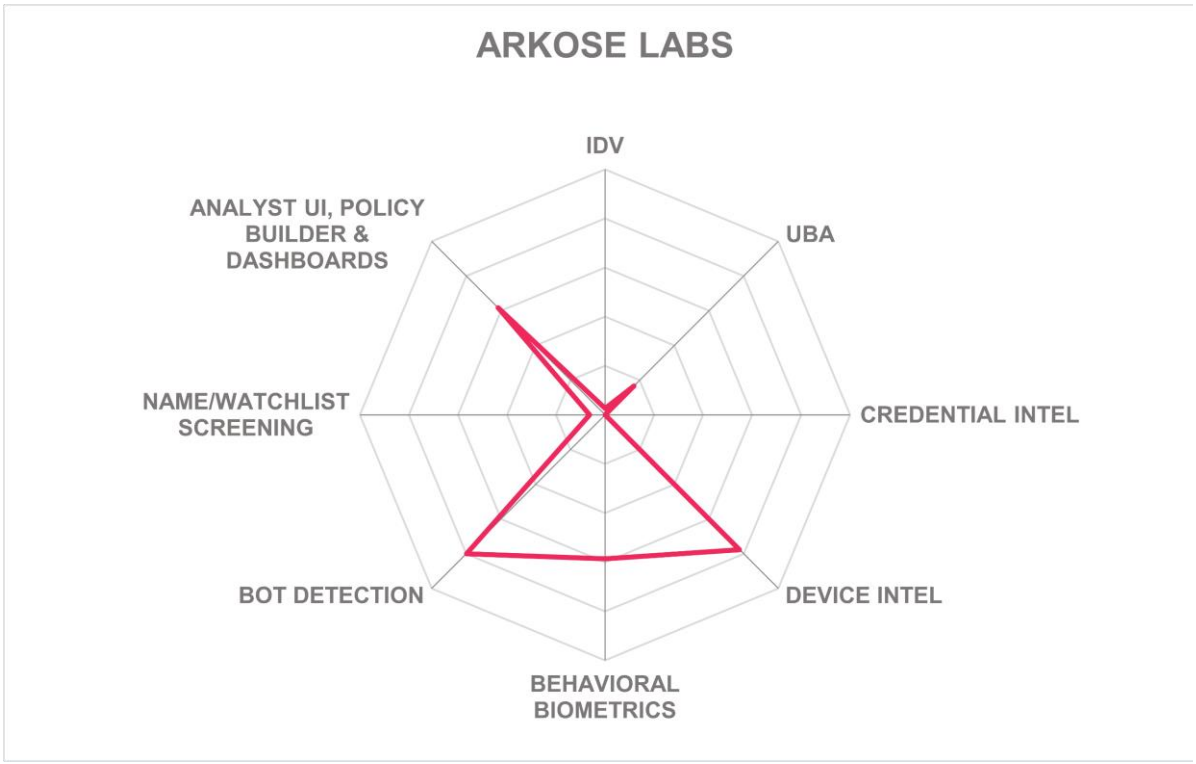
Strengths

- Multiple security certifications.
- Highly scalable and performant FRIP services available globally.
- Documentation, services, training, and support for many languages.
- Fixed fee based on traffic volumes with zero overage protection cost model.
- UBA can help prevent some types of credit card fraud.
- Advanced bot management capabilities are present.
- Uses GenAI for summaries and reports.

Challenges

- Does not have built-in IDV functions; only one third-party connector available.
- Limited ability to detect NAF and crypto/romance scams.
- Lacks support for AML, KYC, and name/watchlist screening.
- Does not look for APP fraud.
- No call center integrations.
- Stronger API authentication mechanisms needed.

Arkose Labs – Device ID and Arkose Phishing Protection



Arkose Labs is a mid-stage startup established in 2016 in San Francisco, California in the US. Arkose Labs has Arkose Bot Manager, Arkose Email Intelligence, Arkose Device ID, Arkose Edge, Arkose Scraping Protection, and Arkose Phishing Protection in their product suite. Their FRIP solution is focused on reduction of ATO fraud as well as inventory hoarding, screen scraping, loyalty card abuse, and fake reviews. Of the six core functional areas of FRIP, Arkose Labs has credential and device intelligence, user behavioral analysis, behavioral biometrics, and bot detection. The service is hosted in public IaaS in datacenters around the globe. JavaScript is used for web interactions, and Android and iOS SDKs are present for customer app integration. The pricing model is based on per-transaction rates.

Arkose Labs contributes to AML compliance by preventing ATOs and AOs. It provides limited support for KYC efforts through its device ID solution, which helps identify returning devices within a user graph, assess risk, and monitor transactions. The platform does not provide KYC questionnaires or enhanced due diligence. It also does not do sanctions or PEP screening or facilitate filing SARs. Arkose Labs does not provide support for EMVCo 3DS 2 or PSD2.

Arkose Labs does not look for credit card fraud, but it detects chargeback/refund abuse in automated payment fraud and mitigates malicious card testing. The platform detects and prevents money mule account creation, APP fraud, and offers phishing protection against advanced toolkit-based attacks. It does not support BNPL fraud or malicious overlay detection. Arkose offers a $1 million warranty.

Arkose Labs does not provide built-in IDV services or interoperate with third-party IDV services. The platform does not evaluate third-party compromised credential intelligence sources, but it does recognize known good users, which helps to eliminate friction for customers and reduce risk. Arkose Labs' platform includes Email Intelligence, which can prevent NAF (and synthetic identity fraud) from invalid email addresses and domains, and it can detect invalid users in popular email providers such as Gmail, and Microsoft Outlook and Hotmail. Email Intelligence interdicts both volumetric and low-and-slow registration attacks. For device intelligence, it examines device IP addresses, reputations, geolocation, IDs, fingerprints, and performs device posture checks. Additionally, Arkose Device ID offers dual device identification methods, leveraging deterministic and probabilistic identifiers, for long-term recognition and to generate updatable session identifiers. It provides data for third-party applications to perform UBA but does not perform UBA itself.

Configurable data retention policies can align with privacy regulations. Their SDKs for Android, iOS, and ReactJS support a limited range of behavioral biometric modalities. Bot detection measures include both activity signatures and behavioral biometrics. One of Arkose Labs' strong points is its ability to deploy highly intuitive and innovative visual and audio CAPTCHAs, and various challenge methods including proof of work. Mitigation methods are configurable by customers. Its device intelligence and innovative CAPTCHAs power its ATO detection and prevention capabilities.

Call center integration is not available. Customers can utilize REST APIs and webhooks, protected by strong API authentication measures, with risk scores and threat categories delivered as JSON. Management interfaces offer detailed reporting, though it lacks ITSM integration. Customers primarily use other products for case management and investigations, with Arkose Labs plumbed into those other tools via API. GenAI can facilitate case description and report generation.

Arkose Labs is ISO 27001/27018 and SOC 2 Type 2 certified. The platform scales effectively, protecting tens of millions of transactions daily using automatic horizontal scaling in IaaS. Their 99.9% uptime SLA and extensive language support enhance usability. Training options include onboarding and workshops. To protect consumer privacy, Arkose Labs uses anonymization, pseudonymization, obfuscation, and encryption. Arkose Labs has customers beyond finance in sectors such as insurance, healthcare, travel, retail, gaming, media, telecommunications, and government. Arkose Labs has excellent ATO prevention and bot detection and management features. Adding IDV connectors, AML/KYC/sanctions screening, and credit card transaction fraud detection features would increase its appeal in the finance industry. Organizations in the financial sector are looking for good ATO protection solutions should consider Arkose Labs.

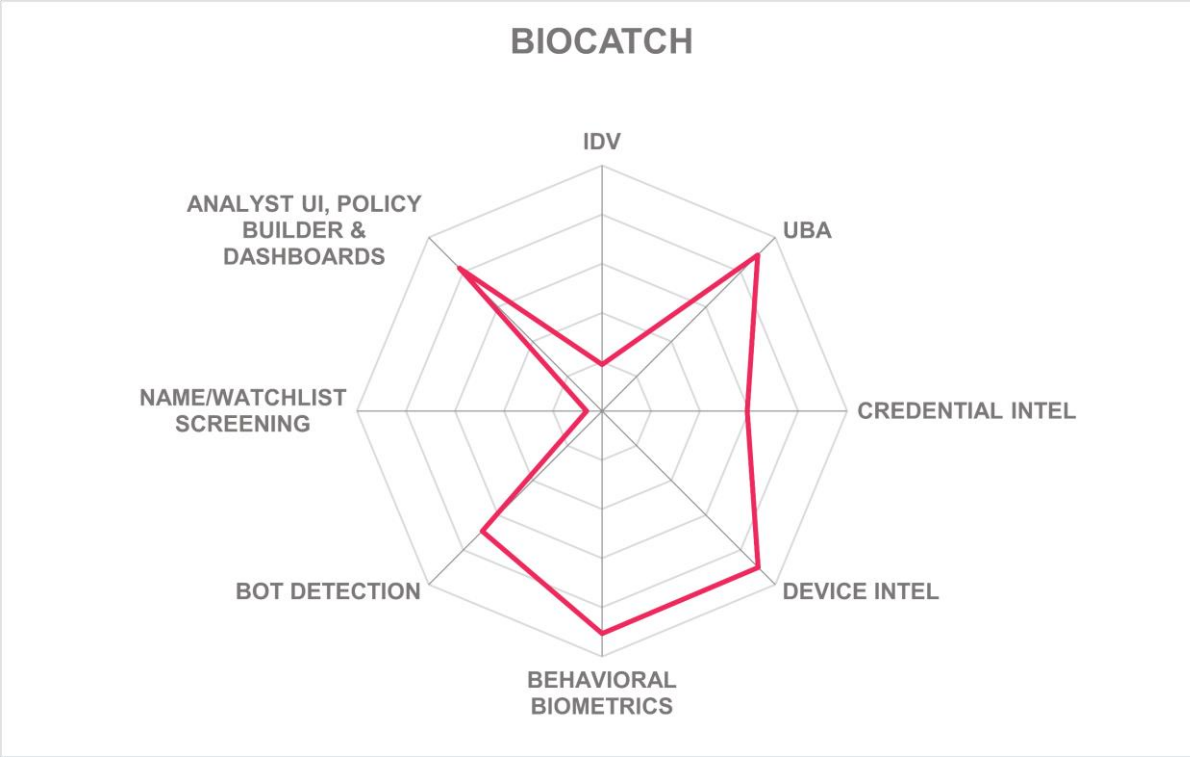
Strengths

- Excellent unobtrusive visual, audio, and proof-of-work CAPTCHAs improve the user experience while reducing fraud.
- Very good bot detection and advanced bot management capabilities.
- Direct integration with popular consumer devices.
- Sophisticated session protection includes TLS fingerprinting and JA3 analysis.
- Improved device intelligence and behavioral biometrics.
- Wide range of industries beyond finance supported.
- Use of GenAI for case descriptions and reports.
- $1M fraud detection warranty.

Challenges

- Lacks IDV features or connections for third-party IDV services.
- Does not use third-party credential intelligence or perform UBA.
- Does not address AML, KYC, or sanctions screening.
- Not focused on credit card or payment fraud; no support for PCI DSS, 3DS2, or PSD2.
- Additional behavioral biometric modalities would be useful.

BioCatch – Connect



BioCatch is a well-funded, late-stage venture-backed FRIP service provider that was founded in Tel Aviv in 2011. They have offices around the world and are focused on risk reduction for financial industry customers. Their suite is composed of modules handling Account Opening Fraud Protection, Account Takeover Fraud Protection, Social Engineering Fraud Detection, Mule Account Detection, Phishing Site Detection, and PSD2/SCA compliance. Of the six pillars of FRIP, BioCatch has device intelligence, behavioral biometrics, UBA, and bot detection. Their service is hosted in multiple datacenters of a single IaaS across the EU, AsiaPacific (APAC), North America (NA), and Latin America. Subscriptions are priced per-user for most components of the suite; and per-transaction for AO Protection and SCA for PSD2 services. BioCatch has partnership arrangements with other FRIP vendors such that BioCatch delivers their advanced behavioral biometrics capabilities through their partners.

BioCatch can stop ATOs, AO/NAF/synthetic identity fraud, APP fraud, BNPL fraud, and the creation and use of mule accounts. BioCatch uses behavioral, device, and network intelligence to understand users' intentions and detect crypto/romance/travel scams and other types of fraud. It can detect the behavior of malware such as malicious banking app overlays and Remote Access Tools (RATs). BioCatch can also deter account creation bots

and credential stuffing attacks. BioCatch does not detect or prevent credit card fraud, chargeback abuse, or card testing.

For IDV, BioCatch relies on detecting behaviors indicative of fraud during account openings, however there are no third-party IDV service connectors, and they do not offer a mobile remote onboarding app for IDV. BioCatch does not have AML or KYC capabilities, nor does it support sanctions or PEP screening. However, BioCatch facilitates SAR by enriching its reports with detection data related to mule accounts. BioCatch Inference Analysis for SCA, when used with MFA, can evaluate how users input passwords and one-time passcodes (OTPs) against their baselines, which serves as a risk factor that can assessed for EU PSD2 compliance. An enhancement to include a possession factor is also expected in 2025.

BioCatch relies on compromised credential intelligence from within their own network of customers but do not engage with third-party sources. BioCatch Connect processes nearly all device and network attributes. It has a new durable device ID feature which remains constant across OS upgrades, thereby reducing false negatives and detecting fake upgrade events. It does not directly detect SIM swap attacks, but it can make inferences and alert customers. BioCatch is working on partnerships with Mobile Network Operators (MNOs) to collect IMEI/SIM and active call information. To counter the proliferation of deepfakes, BioCatch has added some innovative deepfake and virtual camera use detection. BioCatch looks at a long list of login and financial transaction attributes including type, payee, amount, item analysis, velocity and frequency, multiple users per device, proximity to suspicious behavior, and others. BioCatch Trust, a new product in their platform, evaluates risk on the receiving end of customer-initiated transactions by analyzing behavior, device, payment, account, and other signals. It extends protection against hard-to-detect APP scams, such as investment and romance scams, by assessing the trustworthiness of the destination account before a payment is sent.

BioCatch is best known for their behavioral biometrics, which consider a good range of modalities such as keystroke, swipe, gyroscopic, accelerometer, and gesture analysis, supported by advanced ML detection algorithms. BioCatch’s combination of device intelligence, UBA, and behavioral biometrics enable ATO detection and prevention. While BioCatch alerts customers about bots, the solution leaves advanced bot management to customers. The platform allows for configurable data retention policies.

BioCatch Rule Manager enables customers to specify which conditions trigger which actions and simulate rule execution to see the impacts before going live in production. Their risk engine generates granular risk scores and explanatory text output that customer apps can consume. Standard and customizable reports are available. Their APIs support REST with JSON data formats, with a strong authentication option. They have a new fraud analyst and case management interface, which features interactive connection graphs, GenAI augmented event descriptions and a copilot for investigations, video reconstruction of events, and swim lane diagrams for event steps. The BioCatch Case Manager automatically creates and organizes cases for analysts and allows analysts to provide feedback on genuine fraud vs. false positives to fine-tune the detection engine. Integration with ITSM systems and contact center software is not available out-of-the-box.

BioCatch is ISO/IEC 27001 and SOC 2 Type 2 certified. BioCatch operates on a scalable architecture, managing hundreds of millions of transactions daily with SLA uptime guarantees. Training options are available in their support package, and language support is limited to English, Spanish, and Hebrew. They emphasize data privacy using techniques like pseudonymization and encryption, assisting compliance with GDPR and other regional data privacy regulations. BioCatch does not address IDV and credit card fraud use cases but is well-suited for providing advanced device intel and behavioral biometrics for banking, merchants, payment processors, fintechs, and other customers. Organizations in the finance industry will also find their fraud analyst interface to be intuitive and expeditious for investigations.

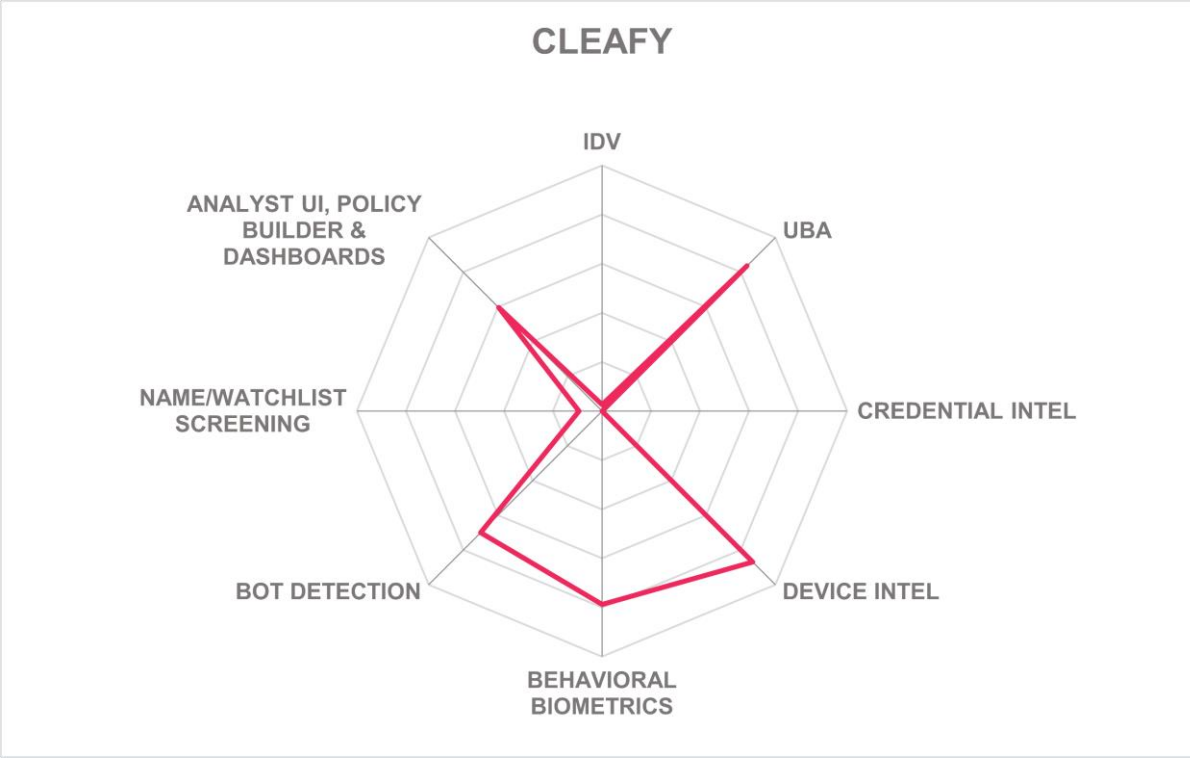
Strengths

- Deepfake and virtual camera detection.
- New capabilities for account reputation analysis.
- Durable device ID which can survive OS upgrades reduces false negatives and can detect fake upgrade events.
- Advanced cognitive analysis for reducing AO fraud.
- Deep transaction analysis.
- Detects ATO, APP, BNPL, mule accounts, and some types of scams.
- GenAI enhanced fraud analyst interface has video reconstructions and swim lane diagrams of events.
- Interactive connection graph expedites fraud investigations.
- Behavioral biometrics aids EU PSD2 SCA compliance.

Challenges

- No IDV features or connectors for third-party services.
- No sanctions/PEP screening; AML limited to mule account detection and account-to-account risk detection
- Does not support credit card fraud detection.
- Lacks call center and ITSM integration.
- Language support could be improved.
- Dashboard customization requires professional services.

Cleafy – Fraud Extended Detection & Response (FxDR) Platform



Cleafy was established in 2014 in Milan, Italy. They also have offices in Colombia, Spain, and the UK. Their FxDR platform is the primary product. It is SaaS, hosted in a single IaaS provider in locations of their customers' choosing. Some customers do run it in their own datacenters or in private clouds. Android and iOS SDKs are available for customer app integration. The solution is priced based on a fixed rate per event per second.

Cleafy provides a degree of AML compliance by incorporating threat intelligence that enables the identification and flagging of known mule accounts across their network of customers and banking partnerships. It does not have KYC features or do any OFAC, PEP, or other sanctions screening. The platform does facilitate SAR filing by automatically linking user and navigation data to enhance transaction monitoring reports. Despite missing support for EMVCo 3DS2, Cleafy aligns with the EU PSD2 RTS by looking for signs of malware and feeding transactional risk data to customer applications.

Cleafy does not currently focus on credit card fraud. The platform addresses financial fraud involving money mule accounts, APP scams, and BNPL fraud using advanced device

intelligence, UBA detection methods, and the aforementioned threat intelligence. Cleafy also detects and mitigates malicious banking overlay apps by analyzing app usage and execution and can detect account creation and credential stuffing bots. It can reconstruct a full user journey in real time, correlate events across sessions, which strengthens detection of sophisticated, multi-step fraud scenarios. It does not look for synthetic identity, government benefits fraud, or crypto-related scams.

Cleafy does not provide built-in IDV services but can orchestrate third-party IDV services through APIs. The platform does not employ compromised credential intelligence but assesses device attributes such as IP addresses, geo-location, device ID, and device type. In addition, the system can detect SIM swap attacks and determine known users on new devices. Their UBA considers a wide range of attributes including login patterns, transaction types, amounts, item analysis, payees, transaction frequency and velocity, relationships to known high-risk accounts, and can infer when multiple transaction attempts from multiple users occur on a single device/IP. SDKs are available for mobile platforms, and obfuscated JavaScript is used for web interactions. Behavioral biometrics encompasses most of the basic modalities plus a few innovative ones. Cleafy's use of device intelligence, UBA, and behavioral biometrics enable it to catch and mitigate ATO attempts. In addition to real-time transaction monitoring, behavioral biometrics is used for bot detection. Bot management is left to the purview of customers.

The risk engine allows for customer weighting of risk factors. REST API and Webhooks are supported, with multiple strong API authentication options. Cleafy has threat and case management modules which are used for investigations; however, the interface needs to be overhauled to improve usability. It does have a GenAI copilot to aid analysts in building queries and to generate case and event descriptions. Standard reports are available, and more can be created as needed. It can interoperate with ITSMs via API, but there are no out-of-the-box connectors. Cleafy lacks direct call center integration and caller ID enhancement but can map call data to user web sessions.

Cleafy complies with ISO/IEC 27001 and SOC 2 Type 2 standards. The platform uses IaaS auto-scaling. Professional support and documentation are available in English, French, Spanish, and Italian. The platform uses privacy-enhancing methods such as encryption, de-identification, obfuscation, and redaction. Adding support for more use cases, such as credit card fraud and scam detection, would make the solution more compelling to other parts of the financial sector. Cleafy's focus on granular UBA for fraud detection is a strong proposition for banks, particularly those in the EU which are subject to GDPR and PSD2.

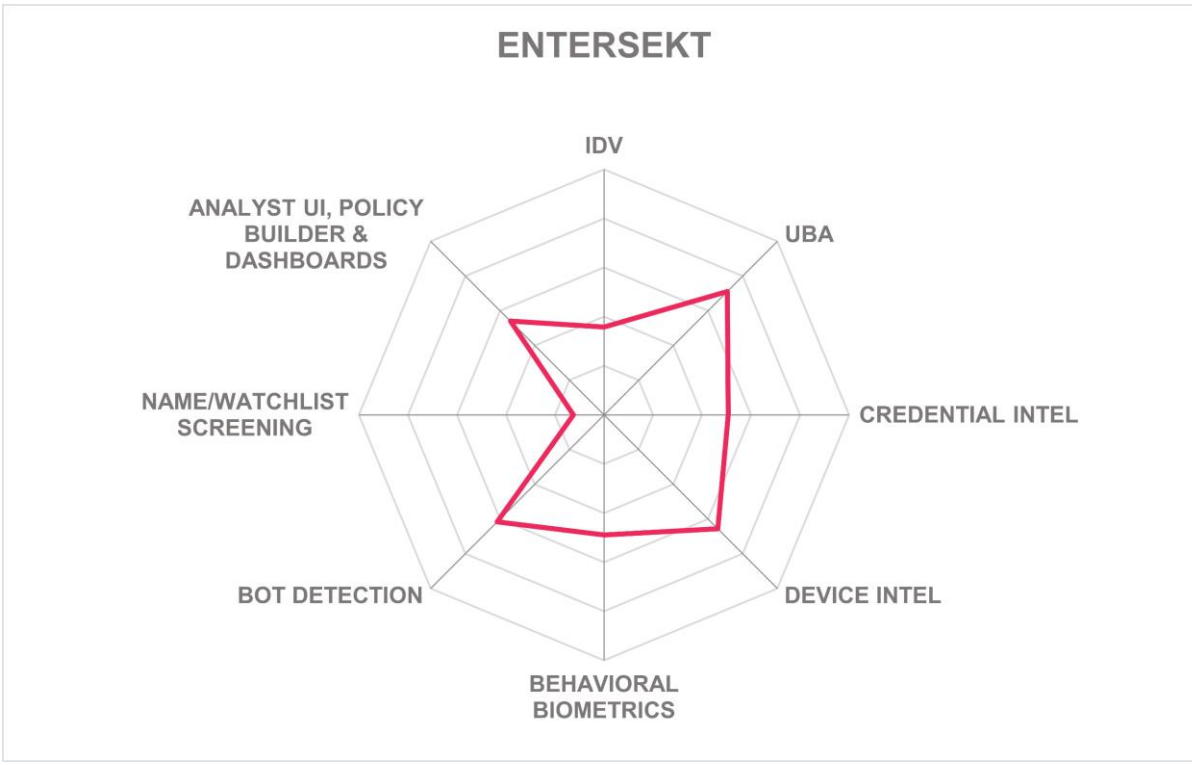
Strengths

- LLM-based copilot can help analysts with investigations and generate event descriptions.
- Fixed fees make it easy for customers to budget for the service.
- Looks for mule accounts, APP, BNPL, and malware.
- Good device intelligence features, including SIM swap detection.
- Uses innovative behavioral biometrics modalities.

Challenges

- Primary interface could be reorganized to make investigations easier.
- No IDV features; does not do name/watchlist screening.
- Not focused on credit card fraud.
- Does not use compromised credential intelligence.
- Device reputation analysis is on the roadmap.

Entersekt – Fraud Extended Detection & Response (FxDR) Platform



Entersekt was founded in 2008 and are owned by private equity. They are dual-headquartered in Cape Town, South Africa and Atlanta, Georgia in the USUSA, and have additional offices in the EU and Asia. Entersekt provides MFA and RBA solutions to digital banks, fintechs, and 3DS issuers. FRIP components include device intel, behavioral biometrics, and a granular risk engine. Entersekt is SaaS, hosted in a single IaaS provider on three continents, with telemetry-gathering functionality delivered via JavaScript and SDKs for Android, iOS, Flutter, and React Native. The solution is priced by numbers of monthly active user devices and per transaction fees. Tiered pricing is available.

Entersekt Authentication Advisor does not assist with AML or KYC compliance, nor does it assist with OFAC, PEP, or other sanctions screening. However, it does provide support for EMVCo 3DS2 by providing risk analysis and authentication for 3DS2 ACS.

The Authentication Advisor detects and prevents CNP fraud by analyzing entity familiarity over time and looking for abnormal transaction requests. It can alert on malicious card testing attempts and chargeback abuse. Entersekt is exploring partnerships that will add money mule account detection capabilities. It addresses APP fraud via call monitoring and

transaction analysis. Synthetic identity detection is accomplished by analyzing patterns and frequencies of appearances of locations of account creation requests and device identifiers. Entersekt can detect malicious banking overlays, rooted/jailbroken devices, and side-car apps. Scam detection is a roadmap item.

Entersekt's solution incorporates IDV services from a single third-party provider, which allows verification through document scanning and facial recognition. It uses in-network credential intelligence and can, upon customer request, plumb in external sources. A long list of device intelligence attributes can be analyzed, including IP, IP reputation, geo-location, geo-velocity determination, network info, device ID/type/fingerprint, and software signatures. However, this analysis is rule-based rather than ML-enhanced currently. Its implementation of UBA enables it to consider login contexts, transaction types, amounts, payees, item analysis, velocities and frequencies, locations, proximity to other suspicious behaviors, and multiple users from a single IP or device. Behavioral biometrics comprise a basic set of modalities. The mixture of device intelligence, UBA, and behavioral biometrics allows Entersekt to deter ATOs. Bot detection is implemented via activity signatures and behavioral biometrics. Bot management is up to the customer application.

Integration with call center application is not available out-of-the-box but can be configured. The risk analysis engine used by Entersekt generates scores and reason codes, and can determine the most appropriate step-up method based on availability and customer preference. The policy building interface is flexible but can be complex. It supports rule simulation against prior transactions to gauge outcomes. It can output decisions as JSON Web Tokens (JWT). REST, Remote Procedure Call (RPC), Webhooks, Websockets, and WebAuthn are supported API types. While case management, ticketing, and basic reports are included in the platform, connectors to third-party ITSM systems and real-time, customizable dashboards are features lined up for future development.

Entersekt is ISO 27001, SOC 2 Type 2, PCI DSS, and EMVCo 3DS2 certified. It uses IaaS auto-scaling and Distributed Denial of Service (DDoS) protection to ensure performance and to safeguard their services. Entersekt has support services and documentation in English and Spanish. Privacy features include regional data storage policies and privacy-enhancing technologies such as encryption, tokenization, and pseudonymization of customer data. Entersekt is targeting the financial industry and has good features for CNP-type credit card fraud detection and transactional risk analysis. Adding capabilities (or integrations) for IDV and scam detection would allow them to serve a broader section of the financial market. It is best suited as a payment services security add-on as part of a larger FRIP ecosystem.

Strengths

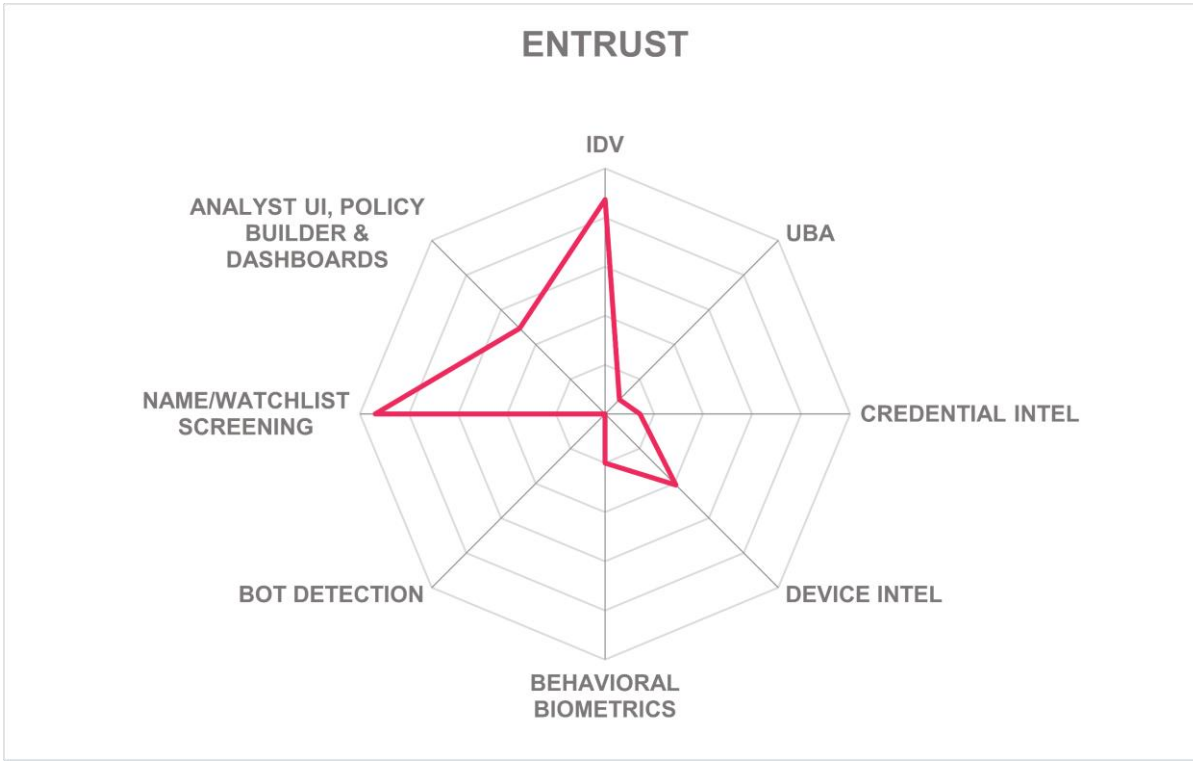
- CNP and APP fraud detection.
- Wide array of device attributes considered by the risk engine.
- UBA examines many transaction parameters.
- Authentication Advisor is a modern passwordless MFA service designed for banks and fintechs.
- Supports CNP fraud detection and does risk analysis and authentication for 3DS2 ACS.

Challenges

- Limited IDV features only provided through third-party integration.
- Not focused on AML, KYC, or name/watchlist screening, nor NAF or synthetic identity fraud detection.

Missing identity graph and device views, but that information is available in reports.

Entrust – Onfido and Citizen Identity Orchestration Platform



Leader in

Entrust is a leader in identity security, its solutions focus on establishing the identity of an individual with their IDV solution, detecting fraud at the beginning of the customer journey and providing step-up authentication for subsequent use cases. Headquartered in Minneapolis, Minnesota in the US, Entrust also has offices in London, Tokyo, Washington, D.C., and other cities around the globe. The company provides identity-based security software and services in the areas of public key infrastructure (PKI), MFA, and fraud detection for those looking to access secure networks, connected devices, or conduct financial transactions. In 2024, Entrust announced the completion of its acquisition of Onfido, a global leader in identity verification and no-code orchestration capabilities. Their FRIP solution backend is SaaS, hosted in public IaaS on two continents, and is deployed to

customers via Android and iOS SDKs. Pricing is determined on a per-transaction basis. Support services are also available.

Entrust has strong capabilities in AML and KYC compliance, offering features like Digital ID Personal Identity Verification (PIV), electronic IDentification, Authentication and trust Services (eIDAS), mobile Driver's License (mDL) compliance, digital signature integration, and third-party data verification. It supports sanctions screening across more than 200 global lists (such as US OFAC and the EU and UN Consolidated Sanctions Lists), monitors PEPs following FATF guidelines, and provides facilitation for SARs, although the solution does not directly create them. Entrust does not address credit card fraud or chargeback abuse. It does look for money mule accounts, BNPL fraud, and synthetic identity fraud.

Entrust has a mobile app for remote IDV which compares biometric attributes with passports, eIDs, and driver's licenses. More than 2,500 document types are supported. This app and SDK feature a number of unusual techniques for liveness detection. Their solution can detect deepfake documents and images and can even tell if the same face or photo has been used for other account applications. It provides detailed guidance to help users with the IDV process for faster and more efficient conversions. Entrust can optionally record onboarding sessions for proof (but this can be omitted in jurisdictions where it is not allowed). It can integrate with any third-party IDV service via Open Authorization 2.0 (OAuth2), OpenID Connect (OIDC), and Security Assertion Markup Language (SAML). All parameters of user registrations are provided in a comprehensive identity report. Entrust does not evaluate compromised credential intelligence, whether in-network or from external services. Its device intelligence features are limited to basic attributes, plus abilities to detect known users on new devices, jailbroken devices, and malware. User behavioral analysis is missing. Behavioral biometrics is not built-in, but customers can use third-party solutions. Device intelligence is the sole capability for detecting ATOs.

IDV and authentication policies are configurable by customers through the Onfido interface, and many templates are available and can be edited as needed. The interface is built on the workflow approach, with sliders for selecting risk factor weights. Entrust automatically checks the workflows to make sure they are consistent and logical. The risk analyses can be packaged in many formats, including JWT claims, OAuth2 grants, OIDC flows, SAML assertions, and HTTP headers. REST, Simple Object Access Protocol (SOAP), Webhooks, Websockets, and WebAuthn APIs are supported, and strong API authentication options are present. There are no connectors for call center software. Case management is not instantiated within the system and there are no integrations for third-party ITSMs.

Entrust's security certifications are wide ranging, meeting standards like FIPS 197, FIPS 140-2, and ISO/IEC 27001. It aids in GDPR, CCPA, and PIPEDA compliance by employing data protection technologies such as anonymization and encryption. Training options are limited, and English is the only language in which documentation is available. Beyond finance, the solution supports industries such as travel/hospitality, gaming, government agencies, and telecommunications. However, this solution is more of an IDV and authentication service than a full FRIP, as it is missing compromised credential intelligence, UBA, its own behavioral biometrics and device intelligence, and bot detection. Banks and

fintechs with requirements for high identity assurance levels that have other full FRIP solutions may find Entrust's capabilities compelling.

Strengths

- Built-in IDV features including remote onboarding app with innovative liveness detection methods for high identity assurance levels.
- AML, KYC, and extensive name/watchlist screening capabilities.
- Can detect mule account, BNPL, and synthetic fraud.
- Conducts deepfake document and image detection.
- Can output risk decisions as JWT, OAuth2, OIDC, SAML, and HTTP headers.

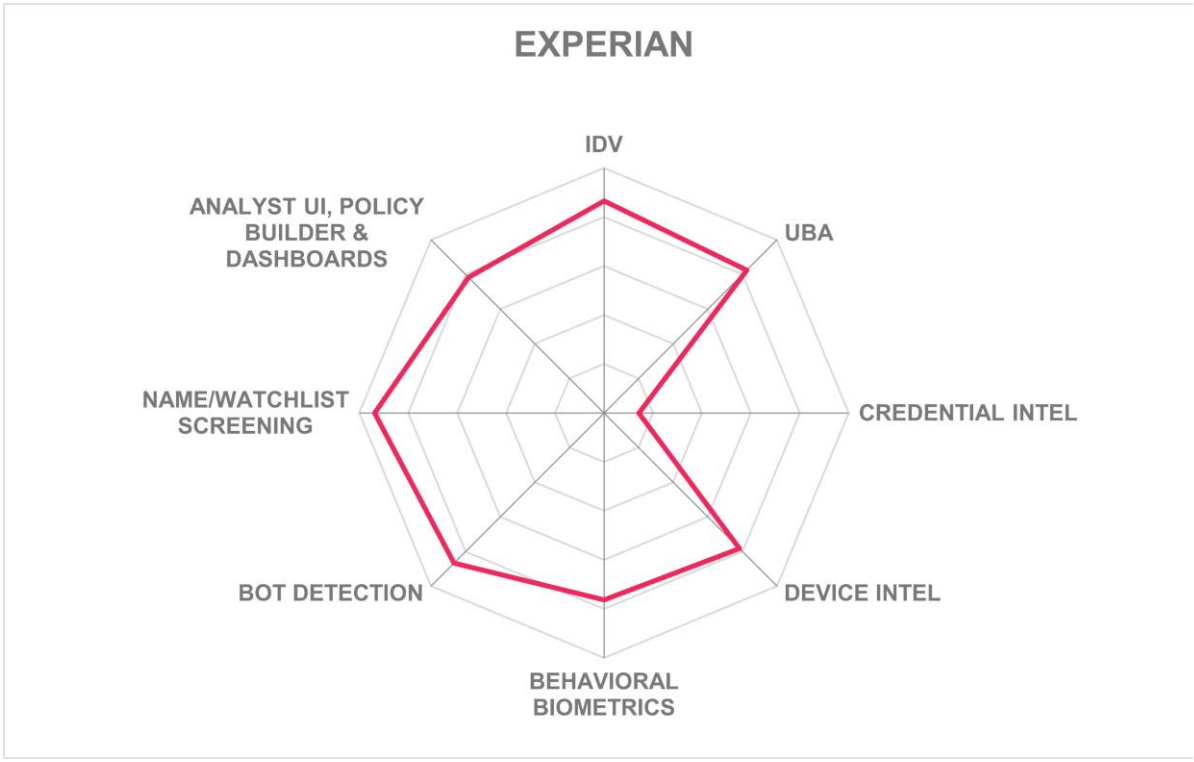
Challenges

- Positioned as an IDV and authentication solution that plugs into more complete FRIP solutions via orchestration.
- Does not leverage compromised credential intelligence or do UBA.

Behavioral biometrics is not built-in, but customers can use third-party products in conjunction with their platform.

- Additional device attributes should be evaluated.
- Does not address credit card fraud.
- Risk engine should be more granular and accessible.
- Only English language for documentation.

Experian – CrossCore on the Ascend Platform



Leader in

Experian was founded in 1996 and is headquartered in Dublin, Ireland. It is one of the “Big Three” credit rating agencies, processing information on 200 million businesses, 10+ billion credit applications, and over 1.5 billion people worldwide annually. It provides credit history information to financial institutions, and analytics and marketing information for other customers. For fraud prevention, Experian has CrossCore, which addresses identity proofing, UBA, device intelligence, behavioral biometrics (via partners), and bot detection. CrossCore on the Experian Ascend Platform, which is a unified fraud, credit, and analytics platform, and is designed to aggregate various fraud sources to consolidate decision making for Experian customers at both account opening and transaction time. CrossCore runs as SaaS in globally distributed datacenters in their own facilities and across multiple IaaS

providers. It can also run on-premises or in customers' private clouds. JavaScript and SDKs capture user information for analysis. Pricing is based on numbers of users or transactions, or numbers of servers (for on-prem and private clouds), and by the types of fraud covered. Bundle pricing is also available.

Experian's CrossCore platform supports AML compliance through integration with PEP and sanctions lists (such as US OFAC, and the EU and UN consolidated sanctions lists) enhanced by proprietary ML models. KYC compliance is achieved using consumer identity data compiled from extensive records. Moreover, Experian offers KYC questionnaires for clients, supports enhanced due diligence checks, and can conduct organizational identity verification through integrations with LEI databases. Additionally, CrossCore enables SAR filing through automated alerts on suspicious transactions.

CrossCore detects and prevents CNP fraud by examining products/SKUs, bill-to/ship-to discrepancies, anomaly detection, and geolocation checks. It can also detect CNR and counterfeit card fraud using device intelligence and behavioral biometrics. The platform mitigates chargeback and refund abuse, as well as malicious card testing attempts. CrossCore can detect money mule account activity, APP fraud, and BNPL schemes. CrossCore can detect NAF and synthetic identity fraud through a combination of identity verification and risk assessments.

Experian provides robust IDV services built into the CrossCore platform, leveraging extensive consumer data as well as integrating with third-party IDV providers. The solution offers a mobile app and SDK for identity document validation (OCR and barcode capture), innovative liveness detection methods, and NFC reads of chipped credentials, offering excellent IDV support for all kinds of consumer-facing organizations. CrossCore does not yet have compromised credential intelligence, but this is on the roadmap. It has thorough device intelligence capabilities, including IP address and reputation, geolocation, geo-velocity, device fingerprinting and posture checks. Their solution can detect evidence of malware and can recognize when a known user accesses a new device. The UBA implementation considers most attributes, including proximity to suspicious events and relationships to known high-risk accounts. Customers can define their data retention policies. Experian's behavioral biometrics can analyze the most common modalities, and customers can utilize third-party solutions as well. The sum of device intelligence, UBA, and behavioral biometrics address ATO detection and prevention. This provides the basis for their bot detection and management functions, thereby allowing customers to maintain allows/deny lists and ban, throttle, or redirect bot traffic as needed.

The platform's risk engine offers graphical visualization and configuration of risk evaluation policies with customizable weighting of risk factors. CrossCore provides non-prescriptive risk assessment outputs to customers to inform their decisions. Results can also be packaged as SAML assertions, JWT claims, or HTTP headers. REST APIs with JSON/XML payloads are supported, and those connections are protected by strong authentication methods. Case management is available in their adjunct products, FraudNet and Hunter. No connectors are available for third-party ITSMs. CrossCore includes limited call center integration capabilities through third-party partnerships. Data can be exported as .csv files, and dashboards are configurable by customers. GenAI assists in creating case and event descriptions, reports,

and interactive query capabilities, in order to expedite fraud detection and management workflows.

Experian has certifications for ISO 27001, SOC 2 Type 2, PCI DSS, and HIPAA. The platform currently handles 8.2 million transactions daily. Customizable SLAs are offered. Experian provides extensive training for administrators and offers support in multiple languages, including English, German, and Mandarin. The product supports many industries beyond finance, such as healthcare, retail, and telecommunications. Experian employs data protection technologies such as anonymization and encryption. Experian, as a leader in all categories, is suitable as a FRIP solution for most financial institutions. FIs looking for a broad set of FRIP capabilities should have Experian on their RFP shortlists.

Strengths

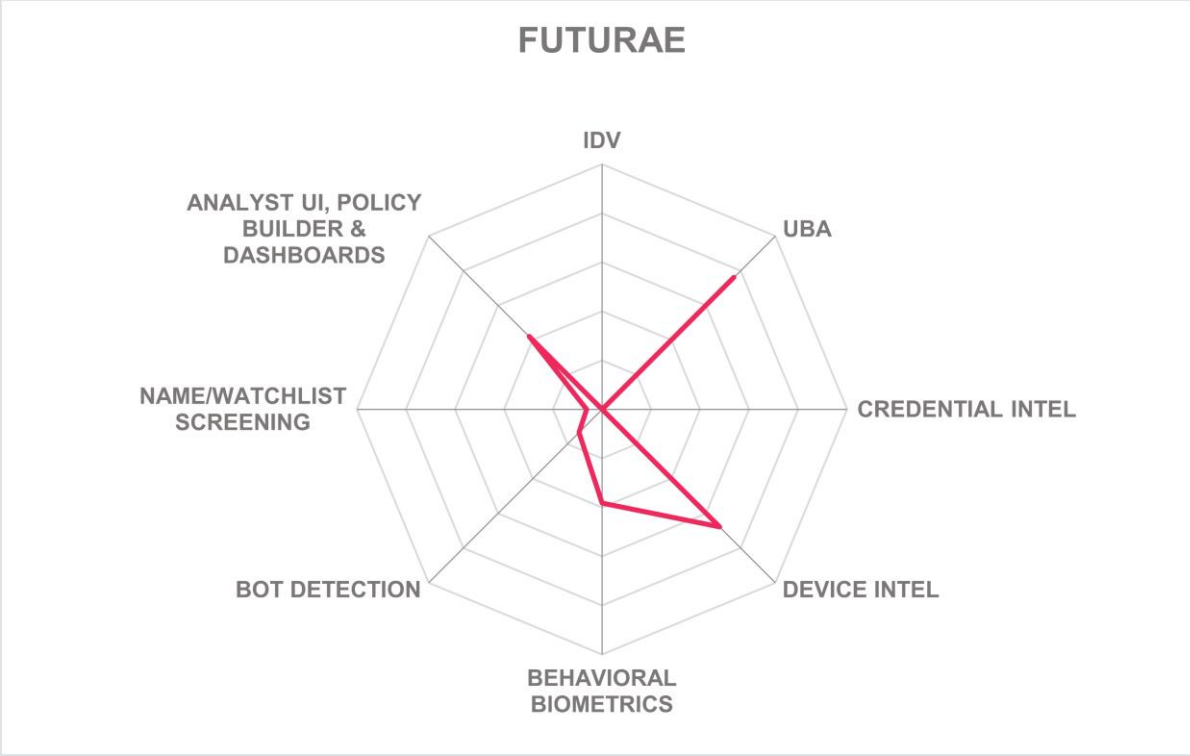
- Excellent IDV features including remote onboarding app with innovative liveness detection features and third-party IDV service connectors.
- Thorough support for name/watchlist screening which enables AML.
- Extensive KYC and KYB features.
- Interoperates with multiple third-party IDV services.
- Authoritative attribute provider for many partners and government agencies.
- Device intelligence encompasses most observable attributes.
- Good support for credit card fraud detection.
- Risk analysis output can be packaged as SAML, JWT, or HTTP headers.
- Many security certifications.

Challenges

-
- Compromised credential intelligence is still in work.
- Webhooks and WebAuthn APIs not supported.
- No ITSM integrations.

Futurae – Fraud Intelligence Platform

FUTURAE



Zurich-based Futurae was founded in 2016. They are a venture-backed startup with passwordless and multi-factor authentication solutions. Their authentication system is an innovation leader in the last edition of the KuppingerCole Leadership Compass on Passwordless Authentication for Consumers. They target financial, payment services, fintech, insurance, and retail customers, primarily in Europe. In terms of FRIP components, Futurae covers device intelligence, UBA, and some behavioral biometrics. The backend service is SaaS, hosted in a single IaaS provider in European datacenters. The client portions are composed of Android and iOS SDKs and JavaScript. Pricing is based on the number of users and transactions processed.

At this time, Futurae does not address AML, KYC, or name/watchlist screening use cases. The authentication solution can be used in 3DS2 flows to supply context to third-party 3DS2 ACS and for SCA and Transactional Risk Analysis (TRA) for PSD2.

For credit card fraud protection, Futurae can detect CNP fraud and device-based insights that may confirm counterfeit/cloned card payment attempts. Their solution can detect APP fraud, and evidence of malicious banking overlay apps.

It does not have IDV features or pre-built connectors for external IDV services, although they could be constructed by customers or systems integrators. IDV solutions are on their roadmap. Thus, it is not designed to detect NAF or synthetic identity fraud and limits the ability to detect mule account money creation. Compromised credential intelligence is not evaluated from either internal or external sources. For device intelligence, IP addresses, geo-location, impossible travel, network context, device ID/fingerprint/type, software signatures, and several other factors are examined, but there are a few attribute omissions. It can detect if devices have been rooted and identify suspicious apps. Its UBA functions look at many user and transaction level details, including login patterns/locations/failures, transaction types, amounts, item analysis, payees, velocities and frequencies, locations, and proximity to suspicious events. It can also discover multiple transaction attempts from multiple users on a single device and relationships to known high-risk accounts. Its passwordless authentication and device intelligence features help to prevent ATOs. Customers can set data retention periods in accordance with regulations and their own policies. Futurae SDKs harvest a small set of behavioral biometric attributes. Bot detection and management are not available.

Futurae delivers risk signals related to authentication and transaction events to customers for evaluation in their Line of Business (LoB) applications or other FRIP solutions. As such, it does not have its own built-in risk decision-making engine. REST API, Webhooks, and WebAuthn (as well as FIDO2) are supported for building integrations with customer applications. The APIs themselves are protected with multiple strong authentication options. Futurae does support packaging of authentication results into JWT claims, OAuth2 grants, OIDC flows, and HTTP headers. It currently lacks dashboards, reports, and case management features. There are no out-of-the-box connectors for call center software or connectors for ITSM systems.

Futurae has obtained ISO 27001 and SOC 2 Type 2 certifications. Support services are available for initial setup, second-level technical support, and incident handling in several European languages. Extensive API-level Documentation and sample code is available in English and modern programming languages. Futurae also provides training for customer admins and developers. Privacy regulatory compliance is facilitated via their use of privacy enhancing technologies such as data de-identification, pseudonymization, redaction, and encryption. Futurae has specialized in transaction fraud detection and behavioral insight generation but is missing several key components of full FRIP solutions as outlined above. Banks and fintechs looking for passwordless authentication solutions with device intelligence and UBA features may want to consider Futurae in conjunction with other fraud prevention solutions.

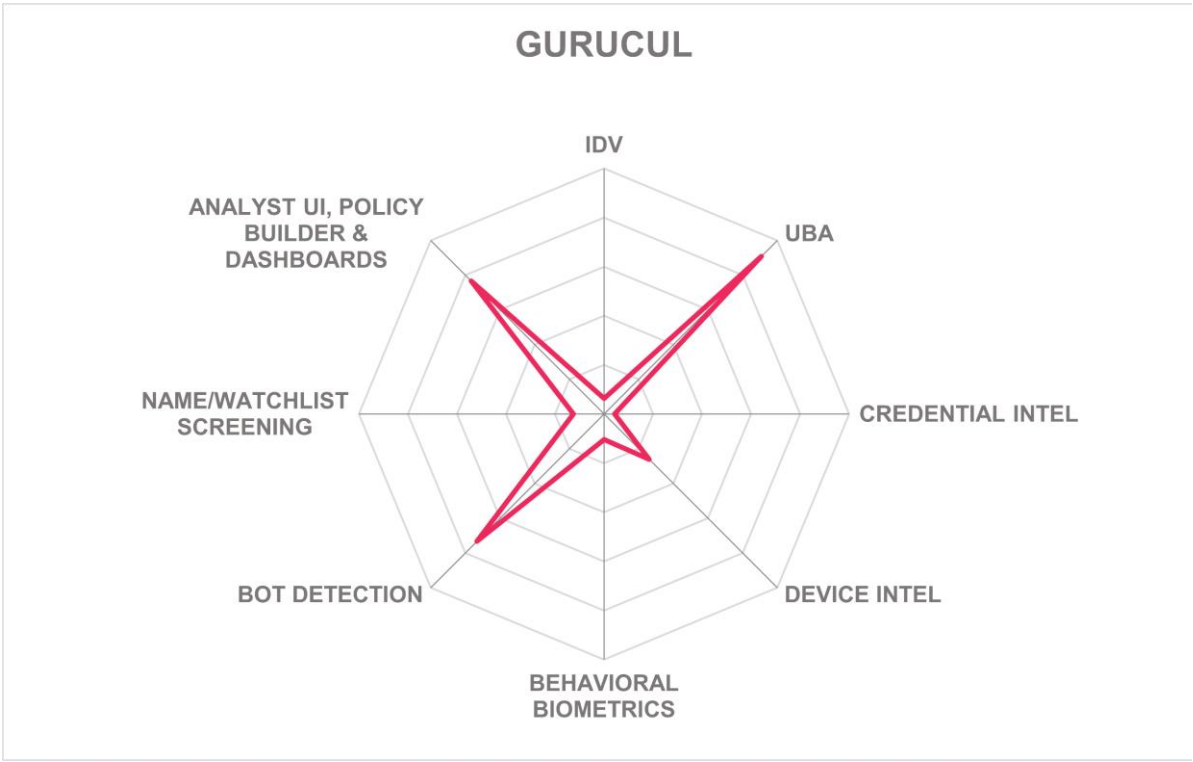
Strengths

- Integrated with an innovative passwordless authentication system.
- Authentication results can be packaged into multiple standards-based formats.
- Looks for CNP fraud, APP fraud, and malicious banking overlay apps.
- Good language support for the region in which it operates.

Challenges

- Not a complete FRIP solution.
- No compromised credential intelligence.
- Lacks IDV services and connectors for third-party providers, but this is on their roadmap.
- Does not support AML, KYC, name/watchlist screening use cases.
- Behavioral biometrics implementation should be enhanced to look at more attributes.
- Does not have a dedicated risk analysis engine.
- Missing dashboards, reports, and case management.

Gurucul – REVEAL Fraud Analytics



Gurucul was founded in 2010 and is a privately owned company headquartered in Los Angeles, California in the US. Gurucul has a suite of products and services including SIEM, UBA, Open XDR, Network Traffic Analysis (NTA), Network Detection & Response (NDR), and fraud and risk analytics. For FRIP components, Gurucul Fraud Analytics platform has credential and device intelligence, UBA, and bot detection. The solution architecture is centered on their data lake and analytics, meaning customers can configure their business applications and third-party FRIP services to gather and send information to Gurucul's Fraud Analytics data lake. Gurucul has hundreds of connectors through which login and transaction data can be imported for analysis. They do not provide JavaScript or SDKs for clients. Gurucul's SaaS runs in a public IaaS provider with global datacenters. The solution can be deployed by customers as VMs or containers on-premises or in any IaaS cloud/environment. Service pricing is based on the number of accounts monitored.

Gurucul does not have built-in IDV features. Integration with third-party IDV services can be constructed via APIs. It can help with AML and KYC compliance via risk scoring of information imported from other sources. It can ingest any name/watchlist and do screening, but customers would have to configure (or purchase) the feeds and construct the logic. If

complete transaction logs are provided, Gurucul Fraud Analytics detects the various flavors of credit card fraud and provide input to 3DS2 ACS and PSD2 SCA systems. It can look for APP, BNPL, and synthetic identity fraud in data from customer transactions and IAM systems.

Compromised credential intelligence is not provided, but customers could configure those feeds and Gurucul Fraud Analytics could evaluate that. Since JavaScript and SDKs are not provided, it cannot directly collect device intelligence or behavioral biometrics; however, it can analyze the common attributes if customers are using other, separately procured sources of device and behavioral biometrics information. This means that bot detection would also indirectly be possible, and bot management would be left to downstream applications. Detection of ATO events by Gurucul is possible but would also depend on third-party product integration. Within Gurucul Fraud Analytics, customers can set data retention policies on imported data to meet their business and regulatory requirements.

Gurucul's competitive advantage is in UBA. It has advanced ML-based detection models that consider a wide range of attributes (if delivered from third-party sources), including login patterns, transaction details such as amounts, payees, locations, times, item analysis, transaction velocity and frequency, identity and address inconsistencies, relationships to known high-risk accounts, and more. Gurucul's risk engine can be tuned by customers via a well-designed interface. Fraud analysts will find conducting investigations is straightforward, starting from the dashboard, or case management and alert screens. Gurucul Studio allows extensive editing of detection models and filters. Call center integration is possible, and there are connectors for multiple ITSM solutions. REST APIs are supported, and results of risk analyses can be packaged into SAML assertions, JWT claims, OAuth2 grants, and HTTP headers.

Gurucul has obtained ISO 27001 certification and is working on SOC 2 Type 2 now. They offer assistance for initial setup and fully managed services. The supported languages are English, German, French, Spanish, Chinese, and Arabic. Privacy regulatory compliance depends on how customer applications are configured. Gurucul Fraud Analytics is powered by its highly flexible and capable UBA functions. It is not a complete FRIP solution, as it relies on external components, including in some cases other FRIP solutions. Organizations that need a good investigative interface or the level of sophistication in transactional risk analysis and scoring may want to consider Gurucul Fraud Analytics in conjunction with other products.

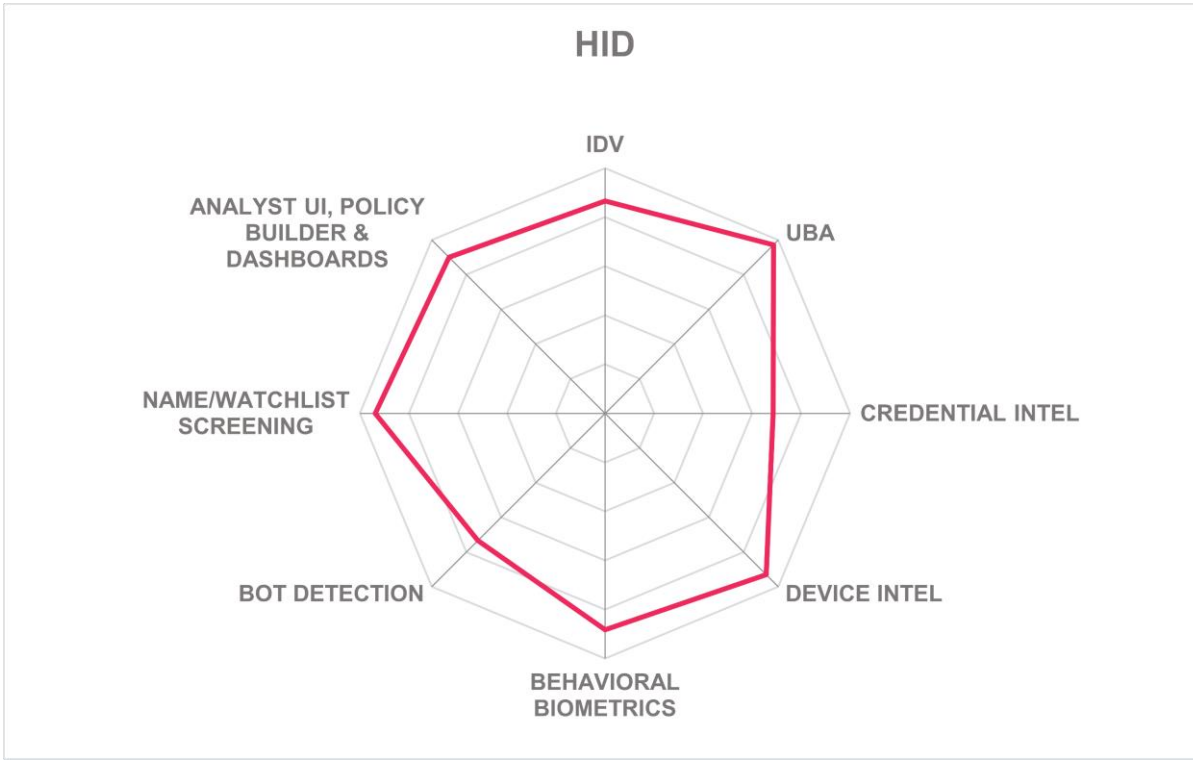
Strengths

- Excellent ML-based UBA functions are applied to transactional risk analysis.
- Hundreds of connectors for third-party security, identity, and LoB/transaction solutions.
- Call center, ITSM, and many other integrations.
- Risk scores can be output in multiple standard formats.
- Gurucul Studio™ allows customers to extensively edit and create new detection models from templates.

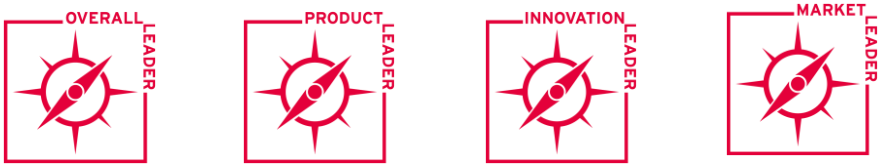
Challenges

- Not a full FRIP solution; does not provide JavaScript or SDKs for telemetry collection.
- No built-in IDV features; connections to third-party services require customization via APIs using graphical wizard-driven processes or professional services.
- Lacks compromised credential intelligence.
- Device intelligence, behavioral biometrics, and IDV are not present, although it can analyze such data if provided by third-party products.

HID – Authentication Platform, Risk Management Solution, Identity Verification Service



Leader in



HID is a subsidiary of ASSA ABLOY Group AB of Stockholm. HID's headquarters are in Austin, Texas in the US. With offices that support more than 100 countries, the company develops highly secure solutions for IAM. These include physical access controls systems, smart identity card manufacturing, credential issuance and management, biometric authentication, card readers, and mobile apps capable of remote identity verification. Their intersection of IAM, biometrics, and SDK allows them to perform identity card issuance for several organizations. The Identity Verification Service (IDV) and the Risk Management Solution (RMS), supported by the Authentication Platform, delivers advanced fraud detection and prevention, which combines ID proofing, credential and device intelligence, behavioral

biometrics, and UBA. The financial industry is HID's main focus. It can be installed on customer premises or in IaaS, and their SaaS is hosted in a Tier 1 IaaS provider in both EU and NA regions. Client-side components are delivered via JavaScript and Android and iOS SDKs. Pricing options include per-registered user, per-server, and per-transaction, depending on the deployment model.

HID has thorough IDV functions that facilitate screening across all major watchlists, which support AML and KYC initiatives. HID Approve supports EMVCo 3DS2 and EU PSD2 compliance and can detect CNP, CNR, APP, and BPNL fraud. Their solution can detect synthetic identities, NAF, and money mule accounts. Moreover, HID can protect government customers against benefits fraud. Together with HID's RMS, it can also be instrumental in detecting crypto, romance, and travel scams and insurance fraud. They have direct integration with some core banking applications.

The HID Identity Verification Service includes a mobile app for document analysis (with more than 7,000 document types supported) and matching as well as facial recognition with passive liveness detection. It can connect with third-party IDV services if needed via API. The solution leverages in-network compromised credential intelligence through HID's RMS. The client-side elements can passively collect the full range of device intelligence attributes, such as location and device type and perform device posture checks, including looking for signs of malware. It can determine if malware is present and if known users are using new devices. HID's UBA is exhaustive, considering login patterns and transaction details such as amounts, payees, items, locations, velocity and frequency, proximity to suspicious behaviors, and relationships to known high-risk accounts. Behavioral biometrics are provided via an integrated OEM partner and the modalities include all the basics plus a few innovative techniques. The ML-enhanced detection features provided by its device intel, UBA, and behavioral biometrics capabilities enable ATO captures. The combination of behavioral biometrics and activity signatures enable bot detection. Allow- and denylisting make coarse-grained bot management possible.

HID's suite can work with call center software, enabling active call detection and providing real-time call risk info to customer fraud analysts. The risk engine allows customers to configure policies easily and set weights on risk factors. API types supported include REST, SOAP, Webhooks, and WebAuthn, and multiple strong API authentication mechanisms are available. Risk decisions can be packaged as JWT claims, OAuth2 grants, and OIDC flows. The system features a visual policy editor for easy rule creation and an intuitive interface that enables fraud teams to quickly investigate incidents through a timeline-based view. Case management is built-in, and connectors are available for JIRA and Salesforce Ticketing. The dashboard is configurable. Many reports are available and more can be created if needed.

HID's SaaS solutions use IaaS auto-scaling mechanisms and are protected against DDoS and protocol-specific attacks. They have achieved a number of security certifications, including ISO 27001/27018, SOC 2 Type 2, and CSA Star Level 2. Training, initial setup, and incident handling are available. Documentation and support are available in English, German, French, and Spanish. HID uses PII de-identification, pseudonymization, redaction, and encryption for privacy protection. Banks, credit card issuers, other financial institutions,

governments, and organizations in other industries should have HID on their shortlists when looking for full-featured, advanced FRIP solutions.

Strengths

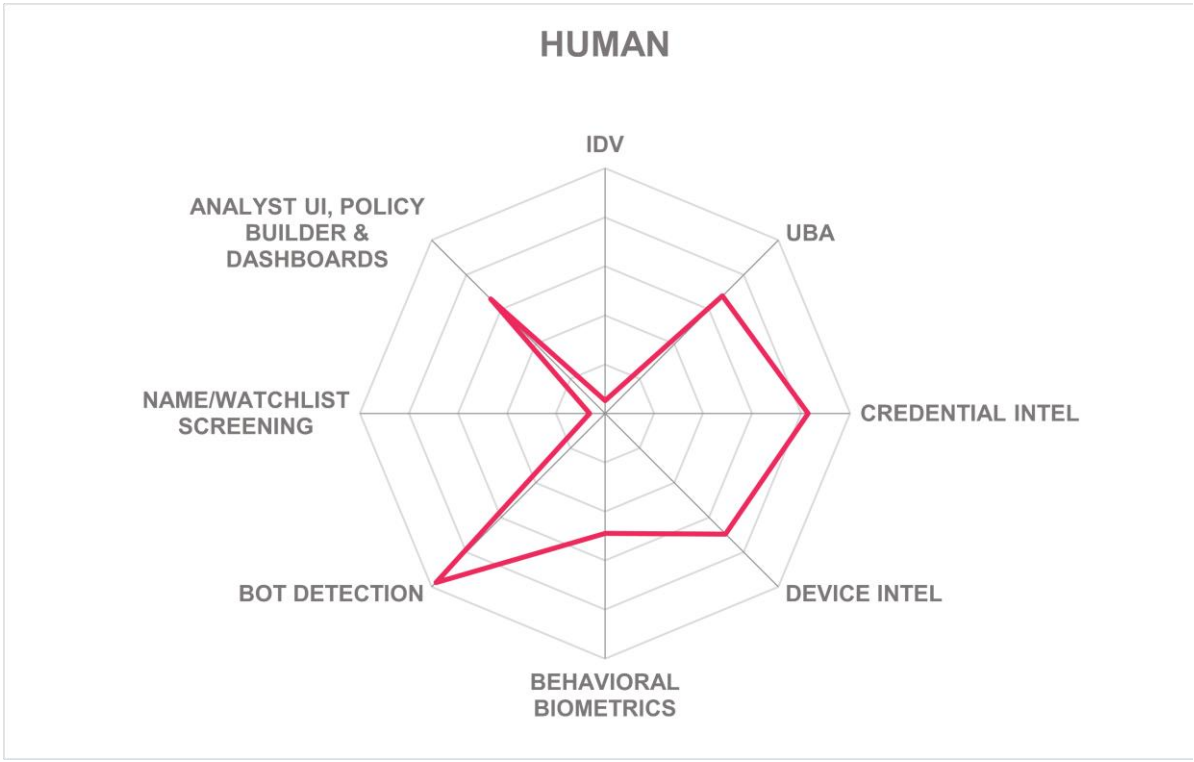
- Excellent IDV functions, including innovative mobile app for remote onboarding.
- Complete sanctions and PEP list screening across all regions.
- Detects APP, BNPL, government benefits and credit card fraud; mule accounts; and synthetic ID fraud.
- Intuitive drag-and-drop flowchart style rule builder.
- Analyst interface pulls together disparate information sources to expedite investigations.
- Examines the full list of available device attributes for superior intelligence.
- Deep UBA functions look at widest range of transaction details.
- Good behavioral biometrics with active call detection for real-time scam detection.
- Delivers risk-based adaptive authentication with a wide range of strong methods, including secure FIDO2 provisioning, device-bound passkeys, and PSD2-compliant SCA.
- Adjusts authentication dynamically to real-time risk signals, balancing user experience with high assurance across possession, inherence, and knowledge factors.

Challenges

- Does not ingest third-party sources of compromised credential intelligence.
- Does not look for chargeback abuse or card testing.

Bot handling limited to allow/denylisting.

HUMAN Security – Human Defense Platform



HUMAN Security was formed in 2012 in New York City in the US and has offices across the US and Europe, as well as in Israel, Canada, India, and Argentina. In summer of 2022, HUMAN merged with PerimeterX, another bot management specialist, and acquired Clean.io, a malvertising protection specialist. The company is privately held and covers many industries including retail, ecommerce, government, insurance, media, SaaS, ticketing, travel, and finance. The Platform is composed of Bot Defender, Account Defender, Code Defender, Credential Intelligence, Media Guard, and CleanAD (for malvertising protection). These products address the credential and device intelligence, UBA, behavioral biometrics, and bot detection and management components of FRIP. The company's Satori Threat Intelligence and Research team enables specialized take-down services. Its Human Defense Platform is hosted in two Top Tier IaaS providers in multiple datacenters on three continents. JavaScript and Android and iOS SDKs comprise the endpoint components. Pricing is based on the number of users for the Account Protection product, and by the number of requests for the Application Protection product.

HUMAN helps with AML compliance by detecting and halting suspicious account activities through continuous monitoring and the automatic flagging of fake, duplicate, and

compromised accounts. This approach ensures that unauthorized credential use is identified and stopped at login, which facilitates ATO detection. The company also supports KYC compliance by ensuring ongoing identity verification via fingerprint and behavioral analytics. Name/watchlist screening is not available out-of-the-box, but customers can download sanctions or PEP lists, import them as .csv files into HUMAN, and write rules to accomplish it if needed.

HUMAN looks for some types of credit card fraud, specifically CNP transaction attempts, and can help prevent chargeback/refund abuse, and malicious card testing by bots. It lacks facilities for detecting APP fraud and malicious banking app overlays but can help identify BPNL fraud. It does not directly discover synthetic identity or NAF but HUMAN can detect fake accounts irrespective of the type of scam with its combination of detection techniques.

HUMAN does not do IDV nor does it have out-of-the-box connectors for third-party IDV services. It uses internal and dark web monitoring for compromised credential intelligence. It evaluates most device attributes, including IP, device type/fingerprint, software signatures, geo-location and geo-velocity, and limited device posture checks. Its UBA surveys many login and transaction details, including types, amounts, item analysis, patterns, proximity to suspicious events, and relationships to known high-risk accounts. HUMAN has behavioral biometrics covering most of the common modalities, and their Satori threat intelligence examines traffic and creates bot activity profiles for detecting them. It does have advanced bot management capabilities, including sophisticated invisible, proof-of-work, and human/non-human CAPTCHA challenges as well as redirection and throttling. The combination of device intel, UBA, and behavioral biometrics help prevent ATOs.

HUMAN's risk engine has a drag-and-drop rule builder that accepts granular conditional logic. Risk factors are tuned by their own internal operations team. The API is REST-based and supports JWT authentication. HUMAN has case management in the dashboard and analyst interface. It can also accept and create cases from email, Slack Connect, and JIRA. Call center software integration is not available out-of-the-box, but customers can use the Account API to retrieve real-time risk info and pipe it into their solutions. A large number of standard reports are present, including customer plots against industry benchmarks. The analyst interface is efficient, with timeline and graph views for easier investigations, and flexible enough to allow customization if needed.

As a cloud-native solution, HUMAN scales linearly according to load. They have achieved ISO 27001 and SOC 2 Type 2 security certifications. Their services are protected against DDoS and protocol-specific attacks. Training and support services are available in English only. HUMAN uses multiple privacy enhancing technologies to protect customer and consumer data, including encryption, de-identification of data, pseudonymization and redaction. In the broader finance industry, banks and fintechs likely need more IDV features than HUMAN has, but organizations that handle credit card payments and/or deal with lots of bot-perpetrated attacks will want to consider HUMAN's platform.

Strengths

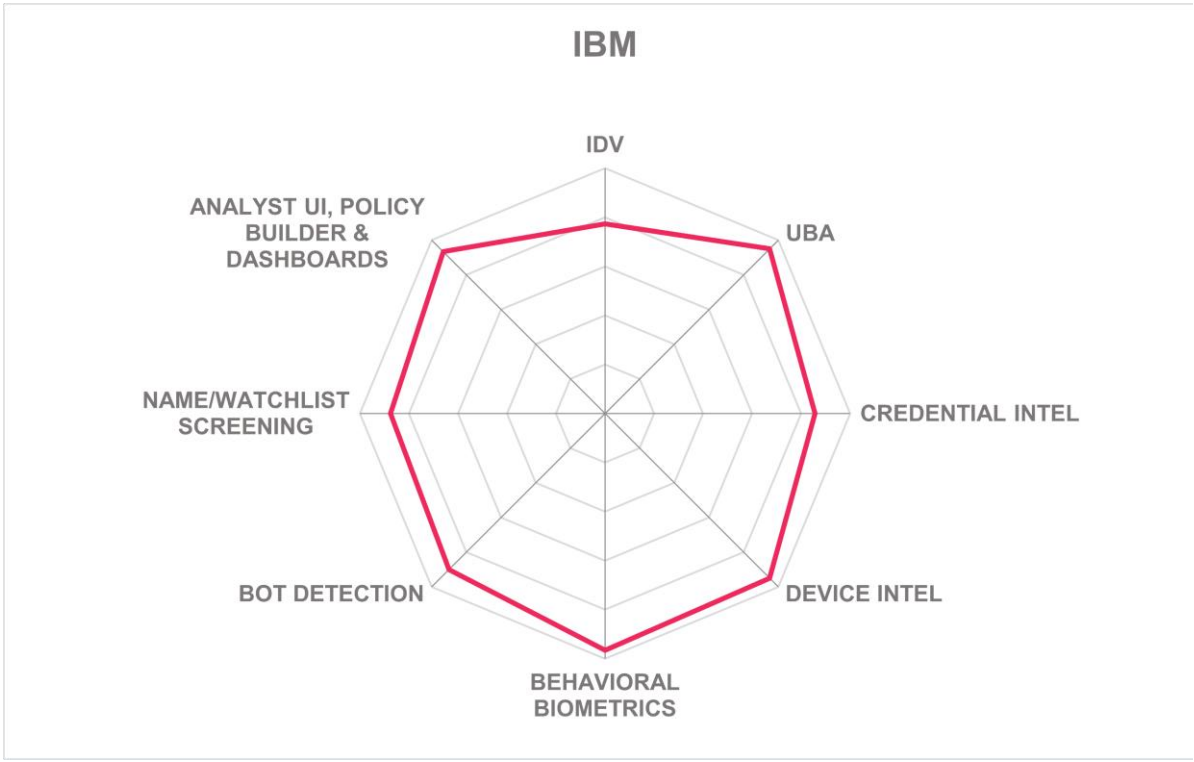
- Looks for credit card fraud and chargeback abuse.

- Can detect crypto, travel, and romance scam types.
- Leverages in-network and dark web research for compromised credential intelligence.
- Bot management options include unobtrusive JavaScript and proof-of-work challenges as well as take-down services.
- Good analyst interface facilitates investigations; the rule-builder interface is flexible and relatively easy to use.

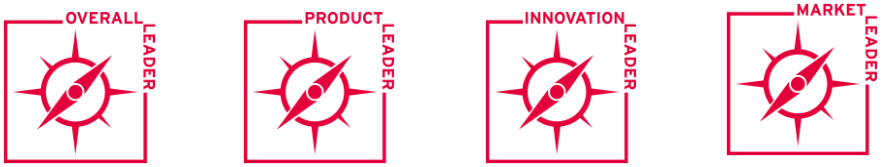
Challenges

- Needs stronger authentication mechanisms for administrators.
- Does not have IDV features built-in; connectors to third-party services need to be configured; limited AML/KYC features.
- Name/watchlist screening not available out-of-the-box but can be manually configured.
- Data retention policies are not configurable.
- Evaluating additional transaction details would be useful for some customers.

IBM – Trusteer: Pinpoint Detect and Pinpoint Assure; and Safer Payments



Leader in



IBM is a global technology and consulting company headquartered in Armonk, New York in the US. IBM offers a broad range of software solutions and infrastructure, hosting, and consulting services in such high-value markets as business intelligence, data analytics, cloud computing, virtualization, and information security. Pinpoint Detect and Pinpoint Assure are the components of Trusteer, IBM's solution for fraud reduction. The integrated suite covers all aspects of FRIP. IBM services are hosted in public IaaS datacenters on three continents. Client-side components include JavaScript, mobile SDKs, and proxies. Pricing options include per-session or by the number of active users.

Trusteer's IDV features help customers with NAF/AO/synthetic identity fraud detection and AML and KYC compliance. Enhanced due diligence for KYC is facilitated through mechanisms that flag risky accounts for further scrutiny. WatsonX can assist fraud analysts with filing SARs. IBM Safer Payments can do screening against any name/watchlist. IBM's solutions can provide risk scores to 3DS2 ACS and PSD2 SCA and TRA.

IBM's suite looks for CNP and CNR fraud, card testing, and chargeback abuse. Mule account detection is facilitated by Pinpoint Assure and Detect and Safer Payments: Pinpoint Assure combines device intel, email reputation, MNO context info, and behavioral biometrics; Pinpoint Detect pulls in mule account characteristics from consortia; and Safer Payments leverages UBA features detailed below. IBM can detect APP fraud via call-in-progress indicators and transaction anomalies, and BNPL fraud at both the time of account opening and when suspicious transactions are attempted. Their solutions can also look for signs of malicious banking overlays and other types of malware. The behavioral profiling engine within Safer Payments detects if users are under duress or if transactions are being initiated under false pretenses. WatsonX AI assistant then can intervene and ask questions of the user such as: "What is the purpose of the transaction?", "How did you meet the person?", "How long have you known them?", "Did they communicate by WhatsApp or Telegram?", "Did they ask you to visit a website or download an app?", or "Were you given a wallet ID?". These measures help shut down crypto/investment and romance scams.

Trusteer has some built-in IDV features, including a mobile remote onboarding app with basic liveness detection, and integrations with Telesign and AWS Rekognition. It uses both in-network and external sources for compromised credential intelligence. Their implementation of device intelligence is complete, covering all expected device attributes, which also allows for SIM swap detection. IBM's solutions excel at UBA, looking at login and a long list of transaction details, including types, amounts, payees, item analysis, velocity and frequency, proximity to suspicious events, relationships to known high-risk accounts, and more. IBM also has very thorough behavioral biometrics, including all basic and some innovative modalities, which inform their bot detection capabilities (along with threat intelligence and activity signatures). Moreover, IBM supports bot management, making recommendations for bot handling to customers over the API, supporting allow- and deny-listing, and redirection. These features combined help prevent ATOs.

The risk engine can be configured by customers, including the changing of risk factor weights. The rule/policy builder uses an older drop-down menu driven approach. A rule simulator is planned. It outputs decisions, granular risk scores, and reason codes. Decision results can be packaged as JWT claims and HTTP headers. It only supports REST APIs, with limited authentication methods presently. IBM's suite can integrate with contact center software and customers can configure connections to ITSM systems. IBM has built-in case management. Many canned reports are available. The fraud analyst interface has a timeline view but no graph view currently.

IBM's services are protected by a Web Application Firewall (WAF) and API security gateways and support rate-limiting. They have obtained certifications for ISO 27001/27017/27018 and SOC 2 Type 2. The solutions also adhere to Digital Operational Resilience Act (DORA), the New York Department of Financial Services (NYDFS)

regulations, and the US Federal Financial Institutions Examination Council (FFIEC) guidelines. As a cloud-hosted service, they use cloud auto-scaling to ramp up to meet peak customer demand. Training and initial setup help are provided, and additional incident handling services can be purchased as needed. The products support many languages. Data is protected using the full gamut of privacy-enhancing technologies. IBM Trusteer and Safer Payments are a solid choice for any financial organization, given the wide range of FRIP features.

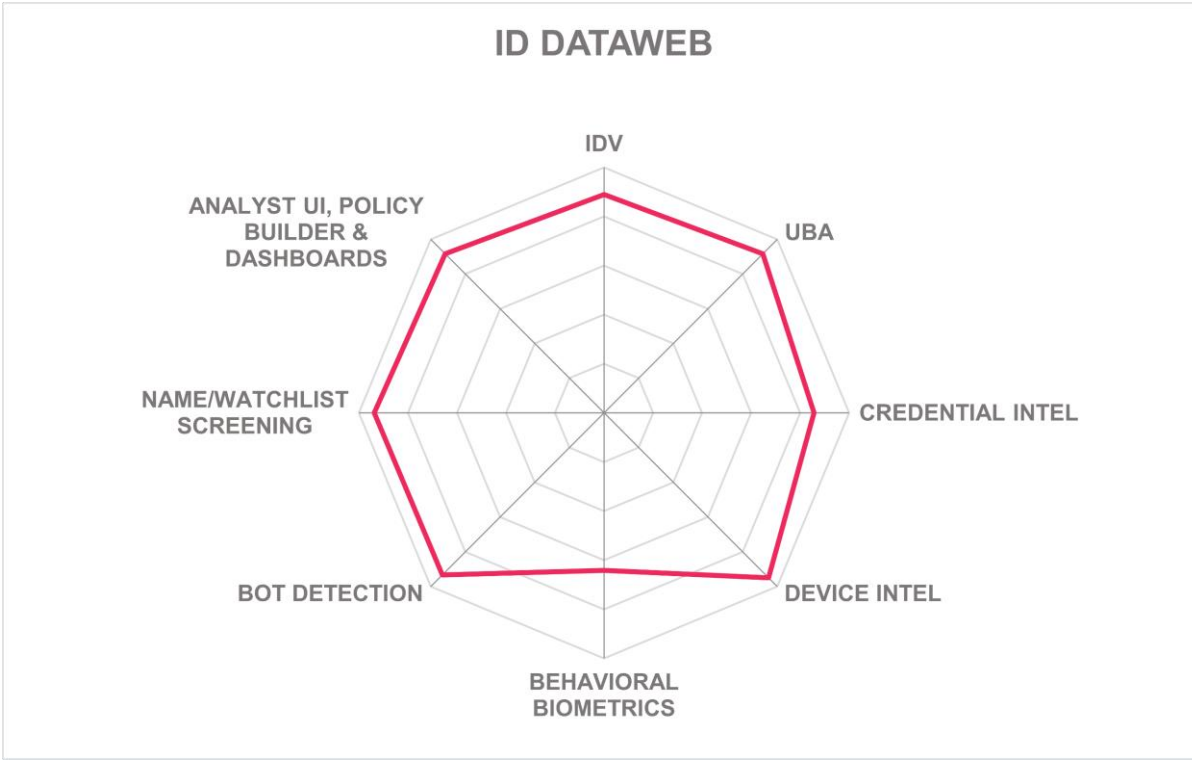
Strengths

- WatsonX facilitates SAR filing.
- Remote onboarding app for IDV.
- Supports credit card fraud detection.
- Deeply granular transaction analysis examines broad range of risk factors.
- Thorough device intel, behavioral biometrics, and WatsonX-powered AI for real-time scam detection and interdiction.
- Excellent behavioral biometrics including some leading-edge mechanisms.
- Bot detection and management are present.
- Innovative use of GenAI for natural language queries, SAR filing, and customer scam prevention.

Challenges

- Additional connectors for third-party IDV services would be useful.
- Additional biometric modalities for liveness detection would enhance the product.
- Policy builder interface needs some updating.
- Support for more API types and authentication methods would increase interoperability.

ID Dataweb – AXN Platform



ID Dataweb was founded in 2011 and is headquartered in Northern Virginia, in the US. ID Dataweb is a late-stage startup that was initially backed by venture capital. The company's Attribute Exchange Network (AXN) product was originally designed to gather authoritative attributes for ID proofing for both government and commercial applications, but the solution now covers all aspects of fraud reduction via orchestration of built-in and OEM'd products. The solution is SaaS-based and is hosted in US datacenters in a public IaaS provider. The client side is made up of JavaScript and SDKs, and they also offer a fully hosted solution based on either OpenID Connect or SAML. This allows easy integration with most identity tools which also support identity standards. Service pricing is per-transaction, depending on the type of attribute services requested.

ID Dataweb helps customers with AML and KYC with their MobileMatch and BioGovID solutions. They have templates for collecting additional PII to meet enhanced due diligence KYC requirements. Their platform can screen against all major watchlists. It supports Legal Entity Identifier (LEI) lookups and ID Dataweb is working on expanding Know Your Business (KYB) features in 2025. It collects data centrally to facilitate SAR filing. It supports

conditional challenges in authentication flows and MFA for 3DS2 and EU PSD2 SCA and TRA compliance.

AXN does not address most credit card fraud types, although clients can set up IDV to reduce chargeback fraud. It does not look for APP, BNPL, money mule accounts, or crypto/romance/travel scams. AXN can detect malicious banking overlay apps, AO and synthetic identity fraud, and government benefits fraud.

ID Dataweb excels at identity verification. It has a mobile app for remote onboarding and IDV that uses leading-edge, iBeta certified liveness detection methods. A long list of third-party IDV sources can be plumbed into registration and KYC workflows. The solution uses internal compromised credential signals and can ingest external sources. Its SDKs, JavaScript, and partner integrations pull in the complete range of expected device attributes for analysis. It can also detect jailbroken devices, known users on new devices, and SIM swap attacks. ID Dataweb performs granular UBA, considering login patterns and many transaction details, including types, amounts, payees, item analysis, velocity and frequency, location, proximity to other suspicious behaviors, multiple attempts from multiple users on the same device, and relationships to known high-risk users. For behavioral biometrics, ID Dataweb uses an OEM'd leading product to evaluate the most common modalities for risk. These functions work together to deter ATOs. Behavioral biometrics plus activity signatures and embedded pixels comprise their bot detection functions. Customers can allowlist and redirect bots, but other bot management functions are not directly present.

ID Dataweb facilitates risk intelligence integration with call center software, including providing caller ID, location information, and carrier information. Moreover, MobileMatch can send OTPs to user devices for real-time proof-of-possession. Other integrations are possible via REST (with strong authentication options), Webhooks, and OIDC support.

ID Dataweb has upgraded its decision engine since the last report. The risk engine can output decisions, risk scores, and reason codes; it can also package results as SAML assertions, JWT claims, OAuth2 grants, OIDC flows, and HTTP headers. The new Just in Time Step-Up authentication feature can inject Dynamic Knowledge-Based Authentication (KBA) and BioGovID requirements into the authentication flow when risk levels are sufficiently high, which helps prevent fraud in financial use cases. The solution provides many templates, and it allows for policies to be constructed via adding conditions and connecting them with logical operators. A flowchart design might make it easier to understand complex policies. Dashboards are configurable, and they enable users to drill down into identity and transaction details for investigations, but it does not have an identity graph view or full fraud analyst interface.

ID Dataweb has garnered multiple certifications, including Kantara NIST 800-63-3 IAL attribute services, ISO 27001, SOC 2 Type 2, and HIPAA. As a cloud-hosted service, they leverage IaaS horizontal and vertical scaling techniques to meet customer demand. Documentation and support are available in many languages. Deployment and incident handling support are provided. They do not store PII and they use encryption for privacy regulatory compliance. Although ID Dataweb does not support credit card / APP fraud and mule account detection, non-card issuing organizations in the financial sector that are

looking for excellent orchestration, built-in IDV, device intelligence, and UBA for transactional risk analysis capabilities should have ID Dataweb near the top of their RFP lists.

Strengths

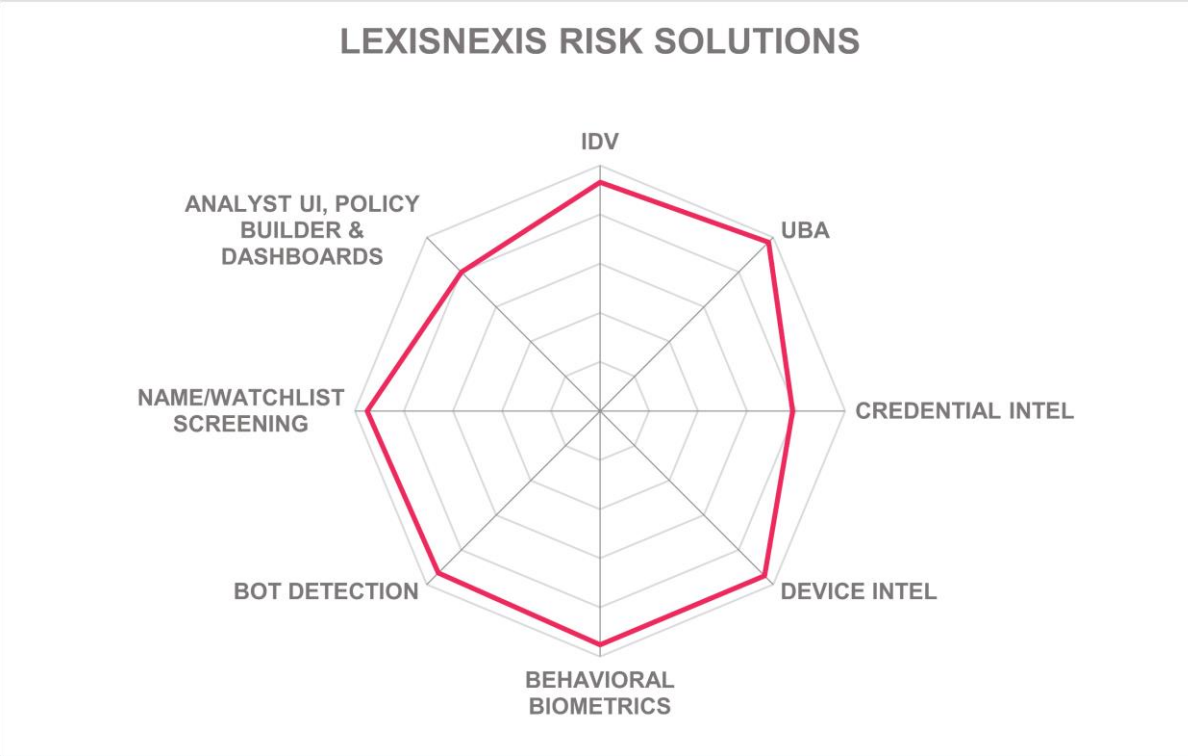
- Excellent IDV features, including a remote onboarding mobile app and SDK that incorporates innovative liveness detection techniques (via partner), and many third-party IDV service provider integrations.
- Support for AML, KYC, and OFAC/PEP/other watchlist screening.
- Enhanced due diligence, LEI lookups for KYB, and SAR filing.
- Call center integration via MobileMatch API.
- Can detect government benefits fraud.
- Very thorough device intelligence capabilities, including SIM swap detection.
- Granular UBA for transaction risk analysis.
- Just in Time Step-Up authentication and/or verification can be added to user journeys in high-risk transactions

Challenges

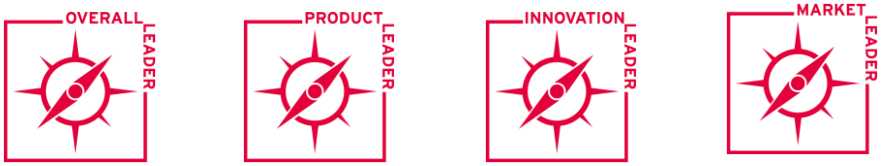
- Does not address most credit card fraud types.
- Does not look for APP, BNPL, crypto/romance scams, or mule accounts.
- Good dashboards but not a complete fraud analyst workbench type interface.
- Although instances could be deployed globally, still only hosted in US datacenters.
- Lacks out-of-the-box connectors for ITSM.

LexisNexis® Risk Solutions – LexisNexis® Dynamic Decision Platform LexisNexis® RiskNarrative® platform LexisNexis® ThreatMetrix®, LexisNexis® BehavioSec®, LexisNexis® Phone Finder, LexisNexis® Fraud Intelligence Solutions Suite, LexisNexis® InstantID®, LexisNexis® TrueID®, LexisNexis® FlexID, LexisNexis® Instant Verify International, LexisNexis® Compliance Lens, LexisNexis® WorldCompliance™ Data

LexisNexis® RISK SOLUTIONS



Leader in



LexisNexis® Risk Solutions was formed in 2000 when it was spun out from LexisNexis, which was founded in 1973. LexisNexis Risk Solutions offers a range of fraud and identity

and financial crime compliance solutions accessible through the LexisNexis Dynamic Decision Platform and LexisNexis RiskNarrative, which contribute to its overall FRIP offering: Fraud Intelligence, InstantID, TrueID, Multifactor Authentication, ThreatMetrix, BehavioSec, Emailage, PhoneFinder, and WorldCompliance Data. LexisNexis Risk Solutions addresses all the major fraud reduction technologies. Its SaaS solutions are hosted in the company's own facilities plus multiple public IaaS providers across three continents. Client components are composed of JavaScript and SDKs. Pricing is based on the number of transactions or API calls plus fees for professional services and tuning, all depending on the combinations of services used.

LexisNexis Risk Solutions provides solutions for watchlist screening, AML, KYC, anti-bribery and corruption, including LexisNexis Bridger Insight XG, LexisNexis Firco Compliance Link, LexisNexis Compliance Lens and LexisNexis Firco Continuity. These screening tools can be used in conjunction with LexisNexis WorldCompliance™ Data, a database of more than 8 million risk profiles including PEPs, sanctions, adverse media, and enforcements. It supports KYB with LEI lookups. LexisNexis Risk Solutions helps customers to file in filing SARs when necessary.

There is a dedicated 3DS2 API for issuers and claim PCI DSS 4.0 certification. ThreatMetrix can detect a broad range of credit card fraud attempts, including skimmed and counterfeit card usage and malicious card testing. ThreatMetrix, Emailage, and BehavioSec work together to detect mule accounts, NAF (including synthetic identity fraud), scams, government benefits fraud, and APP fraud.

LexisNexis Risk Solutions cover IDV in multiple spectrums, including PII-based verification, document authenticity verification, fake identity detection and sophisticated liveness detection techniques to prevent the use of deepfakes. The solution can also orchestrate input from multiple third-party IDV sources if needed. Compromised credential intelligence is evaluated but only from within their customer base, which is quite large.

ThreatMetrix provides exhaustive device intelligence and reputation features, and Phone Finder can provide subscriber information, MNO context, and SIM swap attack detection. Moreover, PhoneFinder can integrate with call center software to deliver this information, plus phone-to-web session mapping, in real-time to help deter social engineering attacks. For UBA, LexisNexis Risk Solutions can evaluate a broad range of login and transaction details, including transaction types, amounts, payees, item analysis, velocity and frequency, locations, proximity to suspicious behavior, multiple transaction attempts from multiple users on the same device, income-to-spending analysis, account creation clusters, and relationships to known high-risk accounts. Its behavioral biometrics capabilities include the major modalities and several innovative ones. These features (from ThreatMetrix and BehavioSec) work in concert to prevent ATOs. Behavioral biometrics, embedded pixels, and bot activity signatures from their Digital Identity Network form the basis of their bot detection functions. LexisNexis Risk Solutions offers limited bot management facilities as well.

The company's risk engine is highly configurable and allows customers to weight the risk factors. Rules can have hundreds of conditions connected by logical operators. Thus, rule editing can be complicated, but they do offer professional services for this if needed. Their

risk engine can output decisions, risks scores, and reason codes. It is accessible via protected REST and SOAP APIs. Webhooks are not supported. It does not support packaging of results as claims or assertions. Case management, dashboards, and standard reports are available. Customizing dashboards and reports requires the company's professional services, however. LexisNexis is testing GenAI but rightfully wants to be cautious about its introduction.

LexisNexis Risk Solutions is ISO 27001 and SOC 2 Type 2 certified. Their services use load balancing and cloud auto-scaling techniques to meet customer demand. Support services are available for deployment and incident handling. Languages supported include English, French, Spanish, and Japanese. Unlike some competitors, LexisNexis Risk Solutions does store consumer data. Consent collection is obtained by their customers. They use de-identification, pseudonymization, obfuscation, redaction, and encryption to protect stored PII. LexisNexis Risk Solutions is suitable for all kinds of institutions in the finance industry, including banks, issuers, payment processors, and fintechs; therefore, organizations in this sector should strongly consider their individual or combined products for fraud reduction.

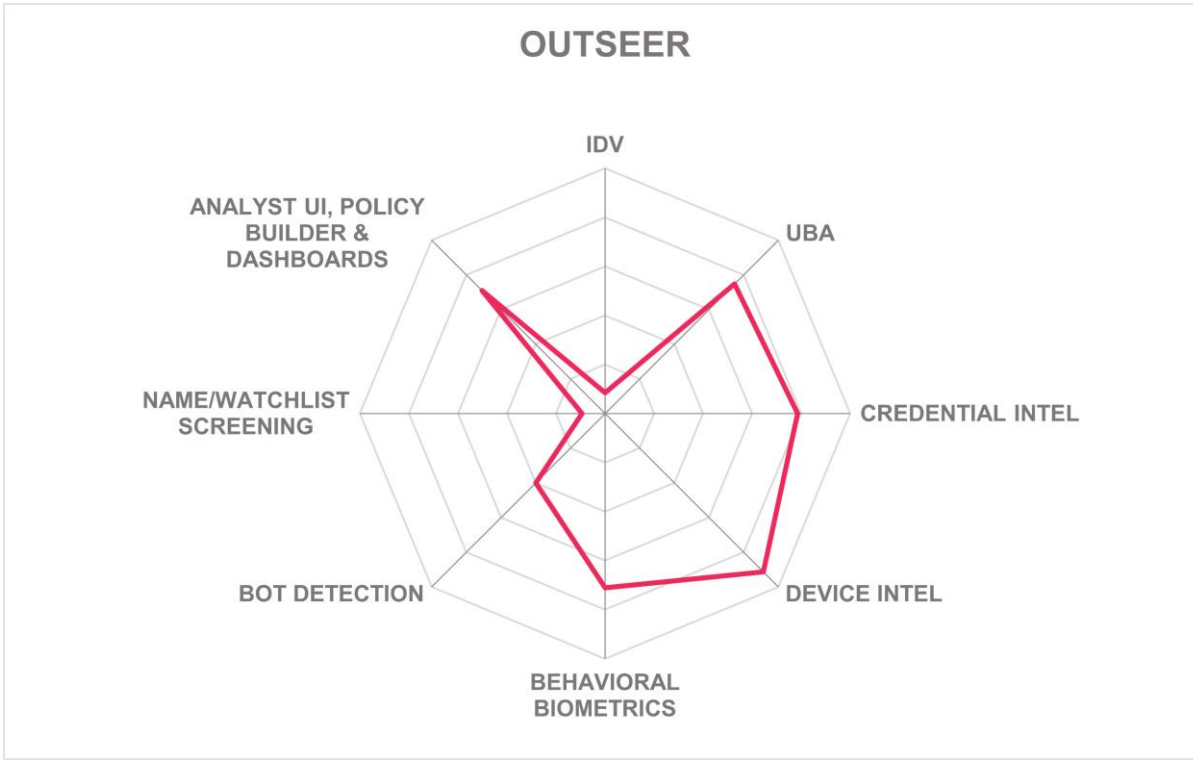
Strengths

- Very thorough IDV functions present, including remote onboarding app with leading-edge liveness detection methods, and integrations with many external IDV sources.
- Deepfake detection is provided.
- Full coverage of credit card fraud types.
- Can detect mule accounts, APP/BNPL, government benefits fraud, and ATOs and NAF.
- ThreatMetrix provides high-quality device intelligence.
- BehavioSec delivers good behavioral biometrics.
- Granular UBA that examines a plethora of transaction details, including some that are not addressed by the competition.
- Customers can train their own ML fraud detection models if desired.
- Rule simulator provides a safe way to view how policy changes would affect outcomes.

Challenges

- Multiple services required for full FRIP functionality; better packaging would make it easier for customers to consume and manage.
- Data retention policies are not configurable.
- Rule builder interface is complex.
- Dashboard and reports customization requires professional services.

Outseer – Fraud Manager, 3-D Secure, FraudAction



Leader in

RSA was acquired by Symphony Technology Group in 2020, and in June 2021 the Outseer brand was launched. Outseer is RSA's rebranded Fraud and Risk Intelligence business unit, and its FRIP offerings are comprised of the products listed above. Outseer is widely used in the financial sector, protecting over two billion consumers. Outseer Fraud Manager can be run on-premises on Linux or Windows with various supporting applications, Outseer Fraud Manager Cloud is hosted in a Tier 1 IaaS in datacenters in the EU and NA, and Outseer 3-D Secure is available as SaaS hosted from their own facilities. The client components are JavaScript and mobile SDKs, which collect device intel and behavioral biometrics. There are three separate solutions within Outseer portfolio: Outseer Fraud Manager, which is widely used to prevent fraud in digital banking; Outseer 3-D Secure, which is Outseer's 3DS ACS

solution for credit/debit card issuers; and Outseer FraudAction, their threat intelligence, management, and takedown solution. Outseer addresses the six core aspects of FRIP, albeit in some cases through integrations with partners as detailed below. Pricing options for SaaS are per-user for the on-premises version of Outseer Fraud Manager, transaction-based pricing for Outseer Fraud Manager Cloud and Outseer 3-D Secure, and Outseer Fraud Action has fixed costs for fraud intelligence feeds and takedown actions can be priced in bundles.

Outseer does not directly provide AML, KYC, or name/watchlist screening capabilities, but customers can import lists and build rules to evaluate the content if desired. Outseer is PCI DSS, and EMVCo 3DS v2.2 and v2.3.1 compliant, providing services for Mastercard, Visa, AmEx, and EFTPOS. Their 3-D Secure product is a 3DS2 ACS, which is designed to protect issuers (but not merchants). As such, it enables credit card fraud protection against CNP, counterfeit card, and malicious card testing. It can also detect ATO attempts and APP and BNPL fraud.

Outseer does not have IDV features, but it has connectors for LexisNexis Risk Solutions, Prove, and Telesign. Thus, it does not look for AO, NAF, or synthetic identities. The Outseer Global Data Network is a repository of compromised credential intelligence that is integrated into Outseer Fraud Manager and 3-D Secure. Moreover, Outseer FraudAction gets additional credential intel from open web, dark web, and social media reconnaissance. This information is shared across their FraudAction customer base. JavaScript delivers thorough device intelligence, including all the common attributes plus device reputation, and malware and jailbreak detection. UBA features examine login and transaction details such as amounts, types, payees, velocity and frequency, proximity to suspicious behaviors such as phishing, multiple transaction attempts from multiple users on a single device, and relationships to known high-risk accounts. Data retention periods are customer configurable in on-premises deployments. Behavioral biometrics includes industry standard modalities and forms the basis of their bot detection functions. Allow- and denylisting are the only bot management methods present.

There are visualizations for risk engine activities via the dashboard, but the dashboard itself is not currently customizable, although there are plans to allow that. The risk engine outputs risk scores and top contributors to the risk scores, and decisions are made within the Policy Manager. It cannot package risk results into claims, assertions, or HTTP headers. Customers can write and edit their own policies, but the policy management interface is composed of drop-down conditions lists that can be combined with logical operators. It could use some revision. It has built-in case management. Each product has its own investigation tool. The products are accessible via REST and SOAP APIs, which are well-secured. Standard reports are available, and customers can export data for consumption and analysis by third-party solutions. Call center integrations are not available.

Outseer’s cloud services take part in annual SOC 2 Type 2 evaluations. Outseer 3DS undergoes regular PCI DSS and PCI-3DS testing. Outseer is in the process of getting ISO 27001 certification. Their solution should support stronger authentication mechanisms. Outseer’s cloud services leverage IaaS auto-scaling for high customer demand. Setup, incident handling, and ongoing support packages are available. Documentation is available

in English. Customers are responsible for data and consent collection, and Outseer uses a wide range of privacy-enhancing technologies to protect it.

Outseer Global Data Warehouse is a new cloud-hosted service that offers premium fraud analytics to customers for additional fees. Outseer also has planned a major overhaul of the risk engine whereby customers will be able to bring their own fraud detection models. Outseer's products are long-established in the market and used by some very large card-issuing clients and banks. It lacks some basic features in IDV that limit its capabilities, and the interfaces are due for upgrades, but issuers and banks will want to consider their feature list when looking for FRIP components.

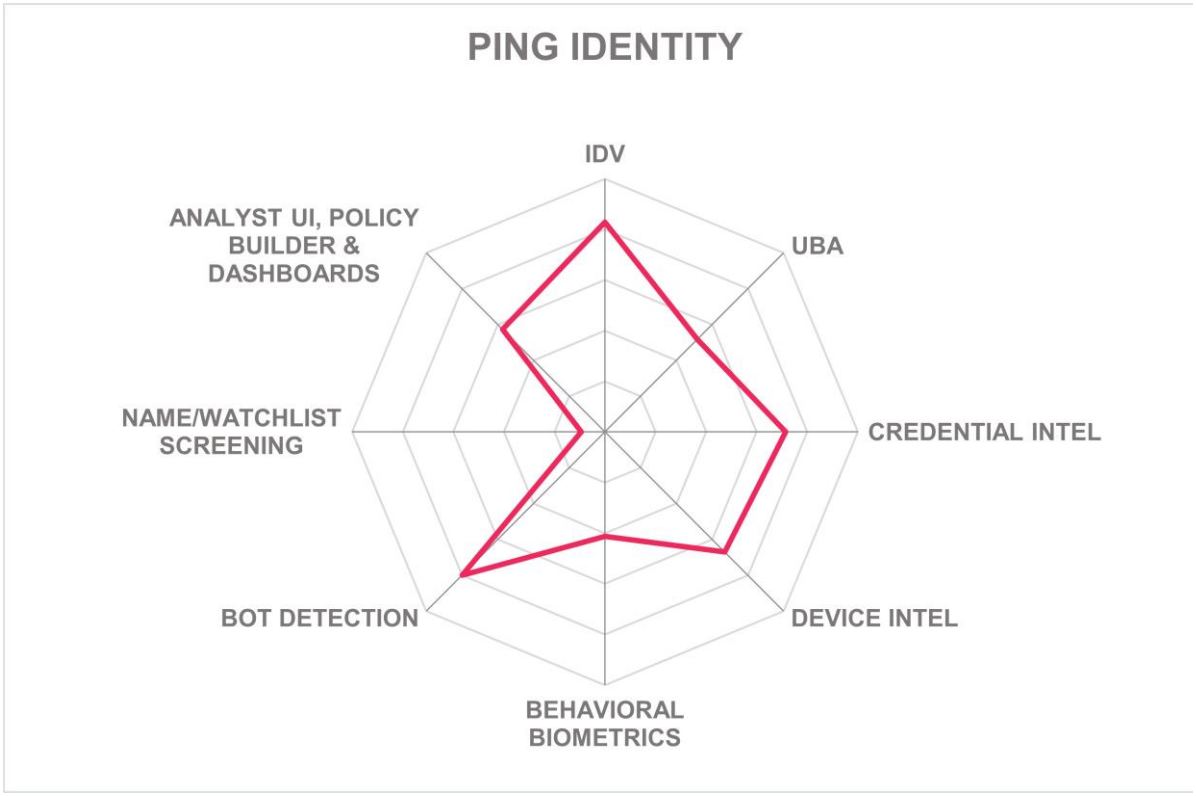
Strengths

- Outseer 3-D Secure is a certified 3DS2 access control server.
- Protects some of the largest credit card issuers.
- Detects ATOs and APP and BNPL fraud.
- Good device intel capabilities.
- Dark web and social media reconnaissance for credential intelligence.
- Fraudster network takedown services.

Challenges

- Needs stronger authentication mechanisms for administrators.
- No built-in IDV functions; a few connectors for third-party services are present but cost extra.
- UBA and transaction analysis should evaluate more risk factors.
- Limited bot detection.
- Rule authoring and investigative interfaces need modernization, and these are on the roadmap.

Ping Identity – P1 Protect, P1 Verify, P1 Authorize, and P1 DaVinci



Ping Identity has been a pioneer in identity federation and access management since its founding in Denver, Colorado in the US in 2002. Ping Identity has grown substantially and went public on the NYSE in late 2019. Ping Identity was among the first enterprise IAM vendors to offer CIAM. Ping's entry into the FRIP space is composed of four products: PingOne Authorize, DaVinci, Protect, and Verify, all of which are part of PingOne Platform. The multi-tenant SaaS versions are hosted in Tier 1 IaaS providers from datacenters on three continents. Telemetry is collected from clients via JavaScript and SDKs. These SDKs are provided out-of-the-box for PingOne Platform customers. Pricing is determined by the number of users and transactions processed.

PingOne Authorize, while not a full AML solution, aids banks by detecting linked accounts and deposits. PingOne Verify provides strong identity assurance for both registration time and ongoing KYC use cases. Customers can insert KYC questionnaires and multiple attribute sources into the KYC workflow with PingOne DaVinci. Name/watchlist screening is not currently supported but is on the near-term roadmap. PingOne is one of the few solutions reviewed that is OpenID FAPI 1.0 Part 2 compliant. The risk-based authentication and risk

analysis features support EU PSD2, and the Neo verifiable credentials (separate product) help with compliance for eIDAS2 and the upcoming PSD3 regulations.

Ping's solutions generally rely on signals from third-party solutions to detect the various types of credit card fraud, which then trigger responses within PingOne components. Mule account detection is only possible with Neo verifiable credentials, so there is limited support for this use case. PingOne Authorize and Protect look for suspicious behavior that indicates APP and BNPL fraud and can require additional IDV or step-up authentication as a deterrent. The solution does not detect malicious banking overlays, but it prevents malicious transactions by requiring FIDO Passkey authentication. It can detect AO, NAF, synthetic identity fraud, gift card cracking, and government benefits fraud through identity verification services orchestrated in PingOne DaVinci. PingOne Authorize can disrupt crypto/romance/travel type scams by embedding questions in the workflow, such as "What is the purpose of this payment – for a friend, a service, tech support?", "Were you called unexpectedly?", "Did it come from a pop-up or email?", or "Did they ask for remote access to your device?", etc. This protects their banking customers by showing that they did due diligence to warn the end user about suspected scams.

PingOne Verify and DaVinci offer excellent IDV features, including a mobile app/SDK for authoritative document attribute scanning, selfie-to-ID document matching, voice verification, and phone/device possession confirmation, with liveness detection that incorporates innovative methods. Moreover, DaVinci allows the inclusion of identity attribute information from a wide array of external sources. PingOne can detect deepfakes during the registration process. In-network compromised credential intelligence is used across the customer base, and individual customers can integrate external sources via DaVinci. The SDKs and JavaScript collect and analyze device intelligence attributes including IP and associated email reputation, device type/ID/fingerprint, and geo-location and geo-velocity. From this analysis, it can identify user and traffic anomalies, device emulators, jailbreaks, and adversary-in-the-middle attacks. It can also infer when SIM swaps occur. Other device checks such as malware detection require third-party integrations. Ping Identity's implementation of UBA considers login times and locations; transaction types, amounts, and payees; and can detect multiple attempts from multiple users on a single device, but does not look at other transaction details. Their behavioral biometrics capabilities cover a subset of possible modalities. The combination of device intel, UBA, and behavioral biometrics enables ATO and bot detection. The solution also has some bot management features including allow- and denylisting and redirection.

The risk engine provides good visualizations of activities via well-designed dashboards, and policies are manually configured in PingOne DaVinci. Most customers use their products in conjunction with other vendors' FRIP solutions, so they do not have a full fraud analyst investigative interface or built-in case management, and report types are limited. Thus, the risk engine yields scores and optional reason codes, but not decisions. Risk evaluations can also be packaged as SAML assertions, JWT claims, OAuth2 grants, OIDC flows, or HTTP headers. REST, WebAuthn, and Webhooks are the supported API types. Access to those APIs is protected by strong authentication methods. Ping's IDV solutions can be used to inform call center software about identity risks, but it does not have call-to-web session mapping. There are no out-of-the-box ITSM connectors.

The cloud-hosted services are protected by defense-in-depth measures, including WAF, API firewall, protocol layer monitoring, and DDoS mitigation. The services are ISO 27001/27017/27018, SOC 2 Type 2, and Tisax certified. Training, documentation, and support services are only available in English. PingOne Platform, as a complete CIAM, does collect and process consumer data. It uses de-identification, pseudonymization, encryption, and redaction to preserve privacy. The dependence on third-parties for credit card fraud detection and omission of certain features in device intel, UBA, and behavioral biometrics are areas for improvement. The lack of a fraud analyst interface and case management would be barriers for adoption for those who need those functions, but not for those organizations who intend to use it alongside other FRIP solutions. Ping's products are well positioned to help customers in banking with IDV and orchestration.

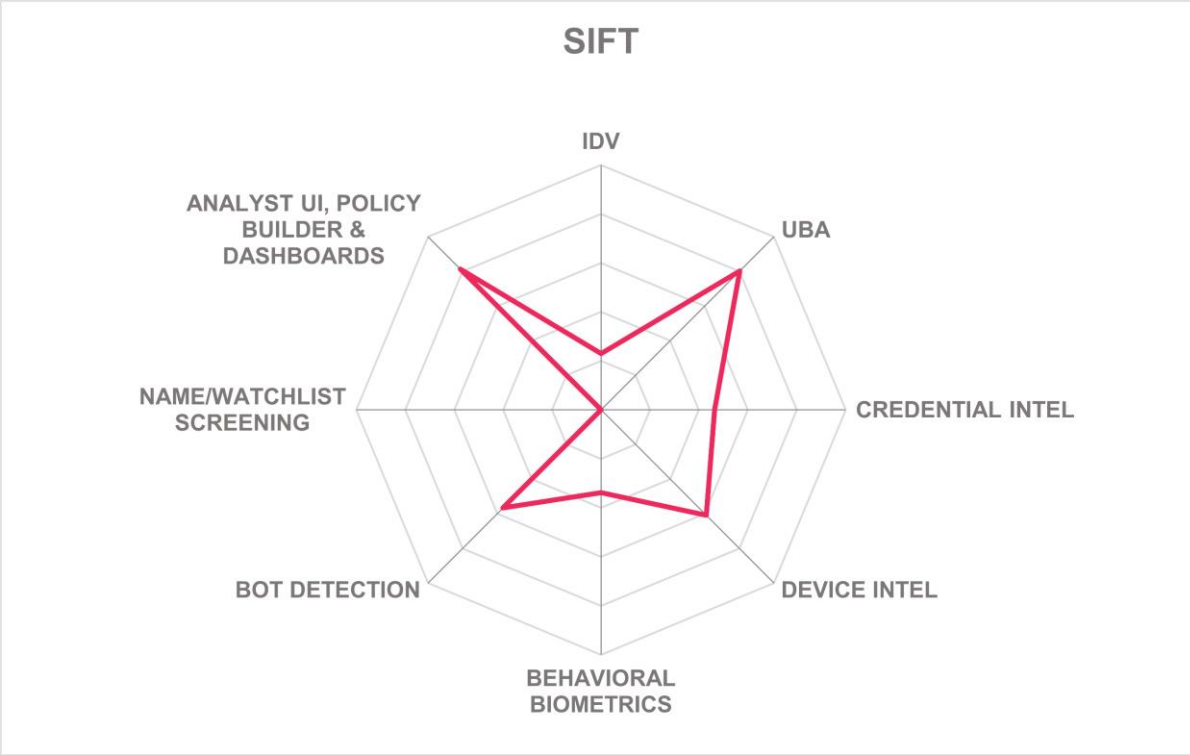
Strengths

- Most flexible deployment options, including SaaS, any cloud, on-prem, and single-tenant instances.
- Deepfake detection during IDV and risk analysis processes.
- Excellent IDV orchestration capabilities, including remote onboarding app with good liveness detection methods.
- OpenID FAPI 1.0 certified.
- Support for EU PSD3 and eIDAS2 (Ping Neo).
- Advanced scam detection and disruption features.
- Many security certifications.

Challenges

- UBA should evaluate more risk factors.
- Behavioral biometrics should consider additional modalities.
- Name/watchlist screening not yet available, but planned.
- Credit card detection requires partner integrations.
- Does not have a full fraud analyst interface or case management.
- Documentation and support are only provided in English.

Sift – Platform



Sift was formed in 2011, and it is headquartered in San Francisco, California in the US. Sift is a fraud protection specialist, with services for preventing AO and ATO fraud, money movement fraud, chargeback fraud, payment fraud, policy abuse, and content scams. Their target customers are in the fintech, ecommerce, dating, travel, and delivery service industries. Areas of FRIP covered by their suite are device intelligence, UBA, behavioral biometrics, and bot detection and management. Their services are hosted in two different public IaaS providers in three different datacenters in the US. Client telemetry is gathered using JavaScript and SDKs. Pricing is determined by the number of billable events, where a billable event is defined as a combination of products invoked and use case, such as logins, orders, account creation, risk scoring, or monthly active users.

Sift does not have built-in IDV features but supports integration with third-party IDV service providers Jumio and Onfido (Entrust). Sift can be called from Ping Identity DaVinci and Okta/Auth0 to provide risk information to help prevent ATOs. Sift utilizes compromised credential intelligence from within their customer base. Sift does not support AML, KYC, or provide name/watchlist screening services. Sift protects the account creation process with its UBA and by detecting device farms and VPN usage, which helps deter synthetic identities

and mule account creation. Its UBA functions can also provide input for 3DS2 and EU PSD2 SCA and TRA.

For device intelligence, Sift evaluates a subset of attributes including IP, IP reputation, geo-location, and device ID/fingerprint/reputation, and can recognize known users on new devices. However, it does not perform device posture checks. User behaviors observed by its ML detection system include login and transaction locations, transaction amounts, types, item analysis, velocity and frequency, proximity to suspicious behaviors, multiple transaction attempts from multiple users on the same device, account creation clusters, and relationships to known high-risk accounts. Sift generates dedicated ML detection models for each customer. Their implementation of behavioral biometrics includes rudimentary modalities and should be expanded. Sift takes a different approach to bot detection, relying on ATO prevention features rather than activity signatures or behavioral biometrics. Bot management is limited to allowlisting.

Sift detects CNP, malicious credit card testing, and chargeback/refund abuse fraud. Sift has automatic chargeback labeling, which creates a feedback loop for Sift's payment fraud prevention solution by automatically updating ML models with chargeback outcomes for more accurate predictions. It can look for APP and BNPL fraud in credit card use cases only. Its behavioral analysis functions enable it to alert on crypto, romance, and travel scams.

The risk engine is customer-configurable. It outputs risk scores but not decisions. Customers can define reason codes that can be returned. REST and Webhooks are the supported API types. The APIs are secured by OAuth2. The Sift Console offers a customizable, widget-based dashboard that provides a view of a customer's fraud landscape, enabling the monitoring of key metrics like blocked users, chargebacks, and automation rule performance. Additionally, Sift provides case management and reports for fraud investigators, offering insights into individual and team case review performance, with capabilities for filtering, exporting, and analyzing key factors such as transaction anomalies and fraud types detected. Sift has recently introduced GenAI features, including ActivityIQ, which summarizes risk patterns across multiple accounts simultaneously.

Sift is ISO 27001 and SOC 2 Type 2 certified. Sift protects against DDoS attacks by leveraging a dynamically scalable load balancer to absorb and terminate malformed requests, mitigates protocol-specific attacks via application firewall rules, and safeguards against API abuse through real-time traffic monitoring, rate limiting, and implementing dynamic deny controls on incoming traffic. As a cloud-hosted service, it uses IaaS auto-scaling features to meet customer demands. Sift offers setup assistance through professional services and guidance from Customer Success Managers. Sift also provides a managed service offering for companies that wish to outsource their fraud prevention operations. Training for administrators is provided during implementation to ensure they are adept at using the platform effectively. Support services are available in English only. Sift uses pseudonymization and encryption to protect customer data.

Sift lacks IDV and name/watchlist screening functions that banks need, but they are more aligned with protecting merchants. Their credit card fraud detection capabilities are useful across many industries.

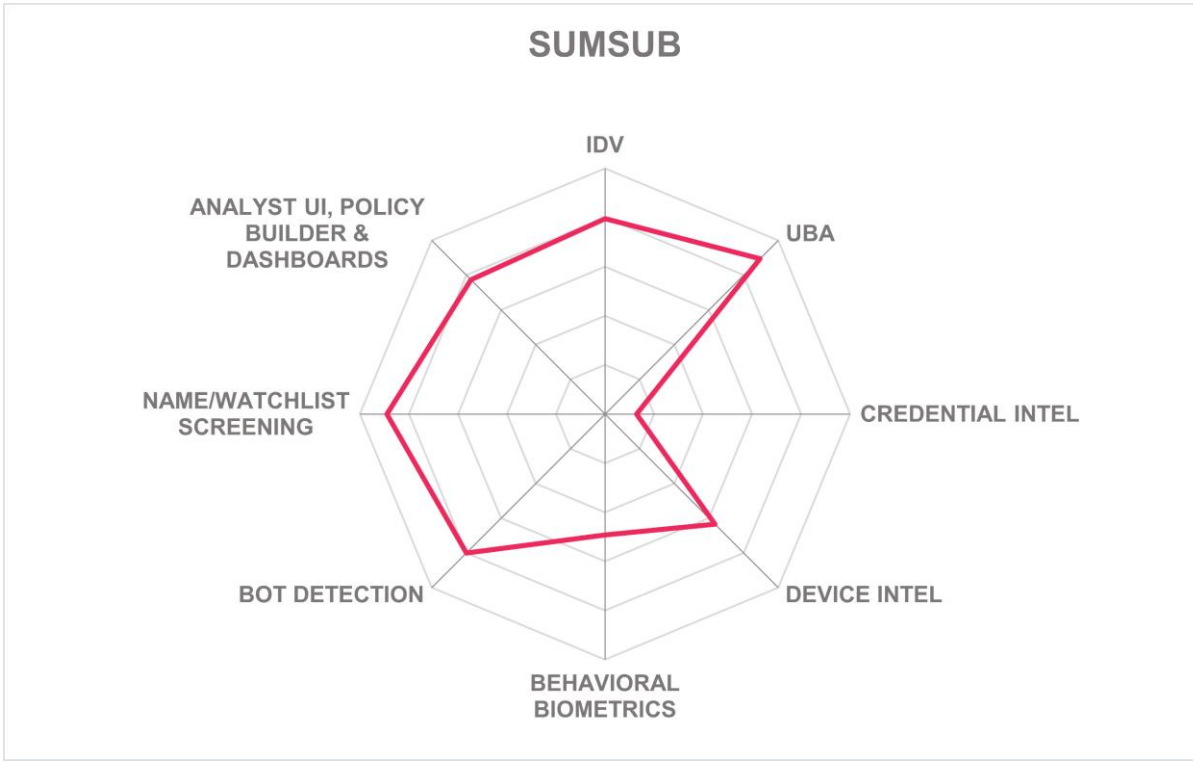
Strengths

- Fraud industry benchmarks available for customer comparison.
- Fraud analyst services for customers who need assistance.
- Good implementation of UBA.
- Bespoke ML detection models for each customer.
- Supports detection of the most common forms of credit card fraud types, scams, as well as chargeback abuse detection.

Challenges

- No IDV capabilities in the platform, but third-party integrations are available.
- Device intelligence and behavioral biometrics capabilities could be expanded.
- Bot detection and management could be improved.
- Only deployed in US datacenters.
- Complex pricing model.

Sumsub – Fraud Prevention



Leader in

Sumsub was established in 2015 in Cyprus. They are a mid-stage fraud protection startup. Sumsub addresses the identity verification, device intelligence, user behavioral analysis, and behavioral biometrics portions of FRIP. The service is primarily SaaS-delivered, but customers can choose to host it in any of the major IaaS providers. The SaaS elements are hosted in datacenters in Europe, Middle East, and Africa (EMEA) and APAC. Client components include JavaScript and SDKs. Pricing models are transaction-based, with charges aligned to the volume of checks performed and discounts for high transaction volumes.

Sumsub’s AML compliance is supported through features such as business verification, transaction monitoring, Suspicious Transaction Reporting (STR) and SAR generation, risk scoring, and AML screening. Sumsub includes support for sanctions screening, encompassing lists such as the US OFAC, the EU Consolidated Sanctions List, the UN Consolidated Sanctions List, and several others from various countries around the globe. Additionally, the solution performs screening for PEPs and against specific blocklists such as the monitorlist and denylist of the international Financial Action Task Force (FATF)s for enhanced security. For KYC compliance, Sumsub can verify age, address, and identity through both document and non-document methods, enhanced by government database checks and video identification. Additional KYC questionnaires can be customized by clients to streamline data collection and risk-scoring as part of user verification workflows.

Sumsub can detect CNP fraud and malicious card testing attempts. Money mule accounts can be identified using device intelligence and behavioral intelligence. APP and BNPL fraud are deterred by device intelligence and KYC challenges. It can detect malicious banking overlay apps. Sumsub can find evidence of crypto, romance, and travel scams with UBA.

Sumsub offers a mobile app and SDKs for identity document validation, selfie-to-ID document photo matching, and liveness detection backed by many innovative mechanisms. Sumsub can also call out to third-party service provider GBG for additional attributes. NAF and synthetic identity fraud can be prevented with Sumsub’s deepfake detection during onboarding. Sumsub does not consider compromised credential intelligence in its risk analyses.

The device intelligence capabilities include checking IPs, VPN detection, geo-location, device fingerprinting, and reputation, but they do not support device posture checks for OS versions and malware presence. Its UBA module considers a wide assortment of transaction attributes such as login patterns, transaction types, amounts, payees, velocities, and relationships to high-risk accounts, multiple attempts by multiple users on a single device, and account creation clusters. Data retention policies are not configurable per customer, but procedures exist to purge data according to region-specific regulations.

For behavioral biometrics, SDKs examine the basic modalities such as swipe and touchscreen analysis and can detect if the user is on a call at the time of transactions, which aids in determining if the user is being coerced. Device intel, UBA, and behavioral biometrics provide the basis for ATO detection. Their Fraud Network Tool looks for connections between users, devices, account creation events, sessions, and network info to detect bots. Allow/denylisting, challenging, throttling, and redirection comprise the bot management options.

Sumsub's risk engine features visualization and configuration of risk evaluation policies for admins, providing risk scores or decisions and text explanations. Clients can customize the weighting of risk factors within policies. Supported API protocols include REST, Webhooks, and OpenAPI, with multiple options for strong API authentication. Call center and ITSM integration are not currently supported. Reports and dashboards feature standard case management and fraud analysis processes, providing reports on case statuses and anomaly detections. GenAI is employed in the fraud analyst interface for interactive NL queries.

Sumsub is ISO 27001/27017/27018 and SOC 2 Type 2 certified. Sumsub employs CDN security services and custom WAF rules for DDoS protection, uses per-client endpoint rate limits, and detects protocol-specific attacks to protect the service from abuse and unauthorized access. Cloud-based elastic scaling is used to meet peak customer demand. Sumsub provides initial service setup assistance and handles incidents on a case-by-case basis. Support services are offered in English, Spanish, Chinese, Russian, and Portuguese, while documentation is available in English and Chinese. Customers are responsible for data and consent collection, and Sumsub uses most available privacy enhancing technologies to comply with relevant regulations.

Sumsub is missing some key features for compromised credential intelligence and bot detection, and its implementation of device intelligence and behavioral biometrics could be expanded to be more effective. Sumsub has good IDV and UBA capabilities that help meet the requirements of banks and fintechs for fraud reduction. Its credit card fraud prevention functions are useful for issuers and merchants. FIs in any region should check out Sumsub's offering.

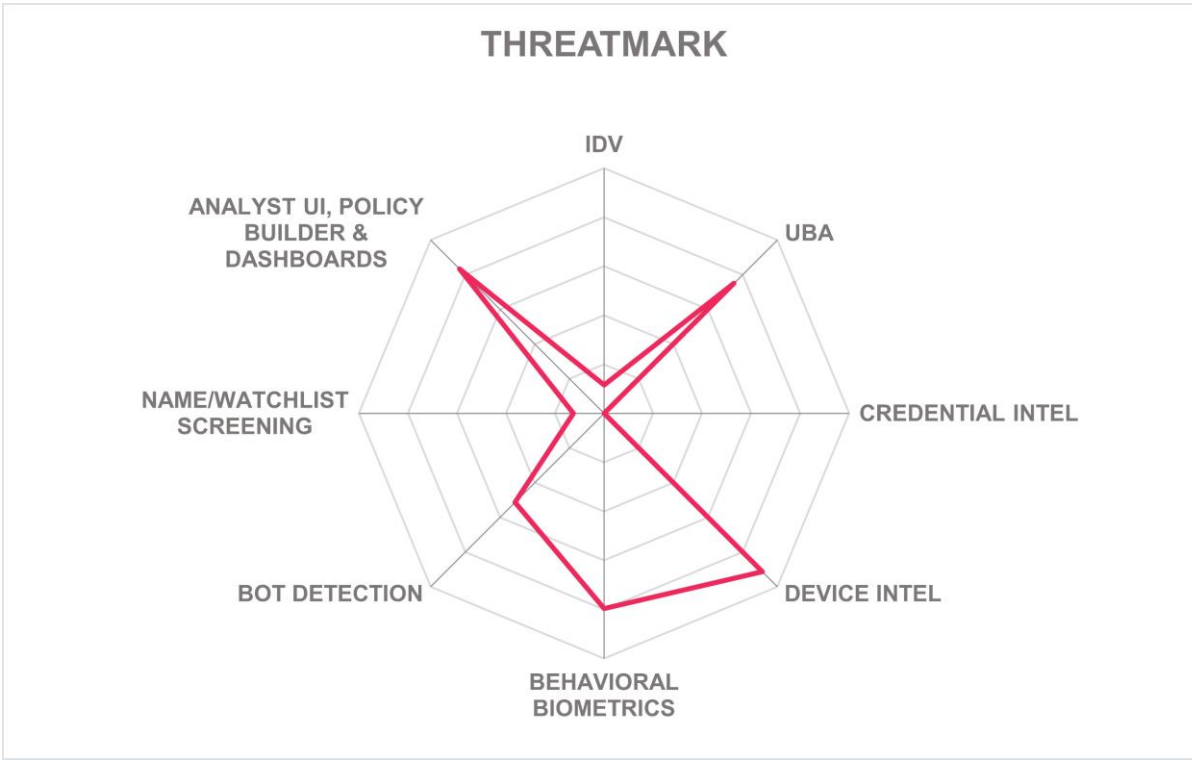
Strengths

- Mobile app and SDK for remote IDV includes many cutting-edge liveness detection methods.
- Excellent coverage for AML, KYC, and name/watchlist screening.
- Detects CNP fraud and some types of scams.
- Deepfake detection is provided.
- Natural language rule builder is available.
- Attack simulator can show what kinds of anomalies to look for per account.
- Has granular transactional risk analysis.

Challenges

- No compromised credential intelligence.
- Data retention policies are not configurable.
- Device intelligence features should consider more elements.
- Behavioral biometrics should include additional modalities.
- Bot detection and management capabilities need expansion.
- Documentation is only available in English and Chinese.

ThreatMark – Behavioral Intelligence Platform



ThreatMark was founded in 2015 and is headquartered in Brno, Czechia. The company is in growing start-up mode and focused on reducing banking and payments fraud. The solution addresses PSD2 compliance, ATO prevention, transaction analysis, and malware and bot detection. ThreatMark has a dedicated SOC and fraud intelligence team to help customers manage incidents. The SaaS solution is hosted in the company's own facilities and in a Tier 1 IaaS provider in the EU and NA regions. Although SaaS is the primary delivery method, the solution can also be run on-premises or in customers' preferred IaaS providers. The client components are JavaScript and SDKs. Pricing is based on the number of active users, where the active user is defined as a user accessing the banking app at least once per year.

ThreatMark does not detect credit card fraud or chargeback/refund abuse. However, it detects and prevents mule account creation and transactions, leveraging user spending behavior and payment data within their shared Fraud Intelligence Network. It detects BNPL fraud through analysis of user behavior and device interaction anomalies. It can help pinpoint scams by looking for increases in amounts and frequencies of transactions to suspicious accounts, and by detecting the presence of remote-control apps. It does not look for AO, NAF, or synthetic identity fraud, but it can detect SIM swap attacks.

ThreatMark itself does not directly perform IDV; however, a couple of FRIP vendors have OEM'd ThreatMark's behavioral biometrics as additional risk signals for their own IDV services. It does not at present use in-network or third-party compromised credential intelligence. For device intelligence, ThreatMark considers IPs, geo-locations, device IDs/fingerprints, network information, OS versions, and device reputations. It can also infer the presence of malware on user devices. Its UBA functions evaluate login frequencies, locations, transaction types/amounts/payees/patterns, multiple attempts from multiple users on the same device, and relationships to known high-risk accounts. ThreatMark helps customers with EU PSD2 RTS requirements with their UBA. Data retention periods are configurable by customers. Its behavioral biometrics modalities include all the common parameters, powered by DL detection models. ThreatMark has a threat research team that develops and refines activity signatures that can, in concert with their behavioral biometrics, detect bots. It also can pose invisible challenges to verify the presence of a human in the transaction. Other bot management features, such as allow/denylisting, throttling, and redirection are not available.

ThreatMark's platform offers support for AML compliance by analyzing user spending habits to help detect fund transfers to suspicious accounts. However, the platform does not help with KYC or name/watchlist screening. The solution does not facilitate automated SAR filing, although it allows for manual export of transaction data.

Their SDK has active phone call and app call (such as Facebook Messenger, Signal, Telegram, and WhatsApp) detection, which is how it can discern if remote control or influence over sessions by fraudsters or manipulation is happening in real-time. It does not have connectors for contact center software, however. ThreatMark's risk engine has graphical visualization and configuration of risk evaluation policies. Customers can configure the weight of risk factors within policies. It supports per-transaction and per-user risk scoring, providing both decisions and risk scores as output, and with optional recommendations for actions based on scores. But it does not support packaging results as claims or assertions. The analyst interface is a modern style, with interactive maps to expedite investigations, and case management is built in. REST and Webhooks are the API types present, although stronger authentication mechanisms should be instituted. Standard reports including case status overviews are available. Integration with ITSM systems is broader than most other FRIPs, with connectors for ServiceNow, JIRA, and BMC Helix.

ThreatMark reports that they have ISO 27001/27017 and SOC 2 Type 2 certifications. Their SaaS uses IaaS auto-scaling features to meet customer demand. Their SLA is lower than their competitors, however. ThreatMark has per-customer API rate limiting. Protection against DDoS attacks is outsourced to the hosting IaaS. Additionally, the system can detect and halt protocol-specific attacks, such as those targeting XML and JSON. Documentation is in English and Czech. Initial setup support is included, and customers can retain on-call security advisors from ThreatMark to help with investigations and to minimize false positives. Customers are responsible for collecting consent from their end-users.

ThreatMark has some innovative features considering their position in the market. They are focused on providing enhanced fraud detection for banks, minus the IDV functions. Their solution is not designed for credit card issuers or merchants. But banks, especially those in

the EU, should take a more detailed look at their UBA, behavioral biometrics, and excellent fraud analyst interface.

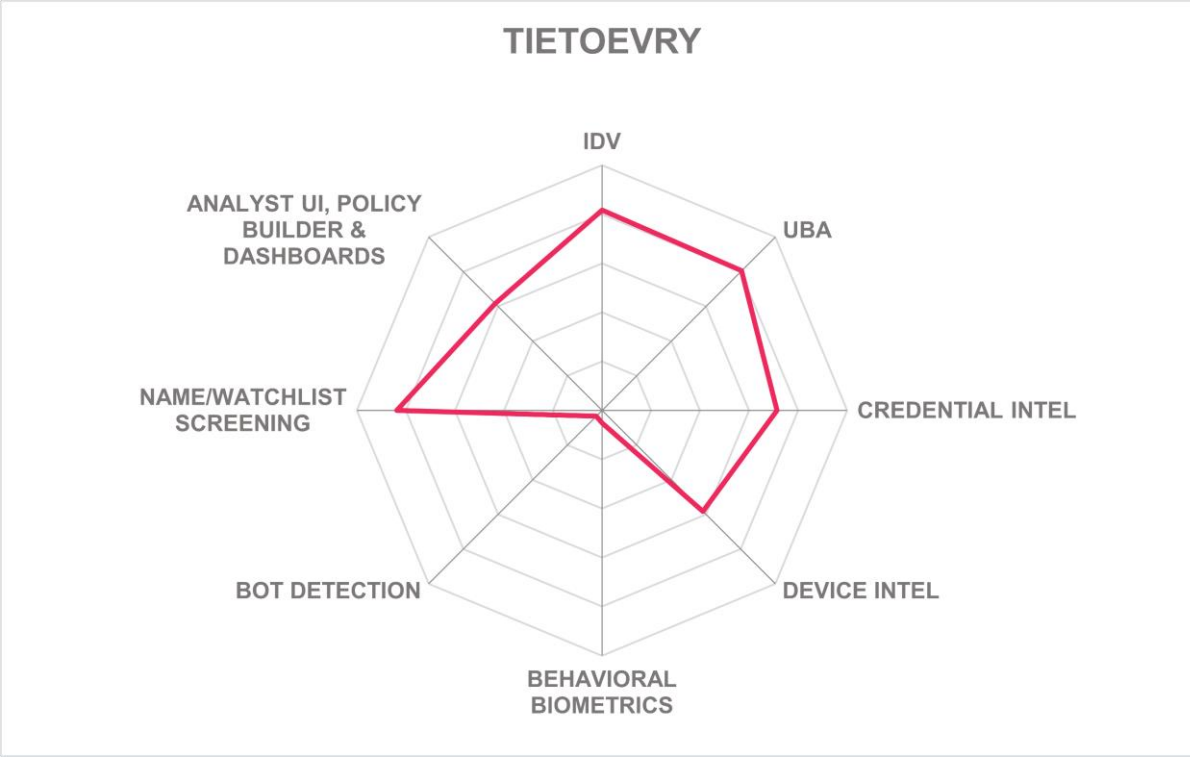
Strengths

- Their technology is OEM'd into other FRIP solutions.
- Can detect APP, BNPL, some types of scams, and SIM swap attacks.
- Innovative DL models used in behavioral biometrics.
- Invisible challenges for bot detection improve the end user experience.
- Integration with key ITSM vendors.
- Very good dashboard and analyst interface for investigations.
- Graphical policy builder in flowchart style.

Challenges

- Does not leverage compromised credential intelligence.
- No IDV functions; does not help with KYC or name/watchlist screening or NAF or synthetic identity fraud detection.
- UBA should look at additional transaction data points.
- No credit card fraud detection.
- Lacks bot management.
- Stronger authentication needed for APIs.

Tietoevry– Financial Crime Platform



Tietoevry Banking, founded in 1968, is headquartered in Espoo, Finland. It is a large, publicly traded enterprise. The company serves a broad spectrum of industries, including financial services, healthcare, manufacturing, energy, public sector, and telecommunications. Tietoevry specializes in consulting, software development, cloud computing, and platform services, providing solutions that support enterprise modernization, customer experience transformation, and secure data-driven operations. The company's portfolio includes enterprise software platforms, managed cloud and infrastructure services, core banking, healthcare, and data analytics applications. Tietoevry has IDV, compromised credential intelligence, device intelligence, and UBA FRIP features. Their SaaS is hosted in a single Tier 1 IaaS provider and in their own datacenters in Norway. The client-side components are JavaScript and mobile SDKs. Identity related services are charged per-user, and fraud detection services are generally priced per-transaction. Fixed price contracts are also offered. They have Business Process Outsourcing (BPO) services for FRIP and identity services that can be contracted separately.

Tietoevry's Financial Crime Platform assists with AML compliance and KYC questionnaires, enhanced due diligence, and verification checks. The platform performs name/watchlist screening against the US OFAC, UN Consolidated Sanctions List, EU Consolidated

Sanctions List, and the UK Consolidated Sanctions List. Additionally, the solution provides PEP screening by examining sources such as Dow Jones and Bogard (now Moody). The platform enables SAR filing to Norwegian authorities.

Tietoevry covers most aspects of credit card fraud detection, including CNP, CNR, counterfeit cards, skimmer identification, and malicious card testing. It does not address chargeback or refund abuse though. To combat money mule accounts, it looks for suspicious behavioral patterns linked to mule operations. For APP fraud, the system proactively identifies suspect transactions, and then their BPO services can intervene to dissuade end users from completing suspicious transactions. Regarding BNPL fraud, the solution detects potentially fraudulent activities by recognizing unusual purchasing patterns inconsistent with the user's past transactions. This solution does not look for NAF or synthetic identity fraud, but it can help detect crypto/romance and travel scams. They also specialize in detecting rogue merchants.

Their IDV capabilities utilize electronic machine-readable travel documents (eMRTD) such as passports and national identity cards, and selfie-to-stored image on chip matching. It uses advanced liveness detection methods instead of the basic types. It also integrates with authoritative attribute sources from the Nordic countries. Tietoevry uses compromised credential intelligence from within its network of customers and from the Nordic Financial CERT. For device intelligence, it examines most of the common set of parameters plus device posture checks, known user on new devices, jailbreak detection, and some malware detection. Its UBA considers login and transaction details including locations, transaction types/amounts/payees/item analysis, velocities and frequencies, multiple attempts from multiple users on the same device, and relationships to known high-risk accounts. UBA and device intelligence enable ATO detection. Behavioral biometrics is not currently available; therefore, bot detection is limited to relying on UBA. Bot management is not provided.

The risk engine can output scores with advice or decisions over the API, but it does not allow packaging of results as claims or assertions. It can provide input to 3DS2 ACS and context for EU PSD2 SCA and TRA. Policies are configurable as needed, but the policy authoring interface is quite complex, with many drop-down selectors and filter settings. Their BPO team helps customers write and edit policies as needed. API types supported include REST, SOAP, and Webhooks. Additional API authentication methods should be supported. The analyst interface is geared toward investigating credit card fraud. It is less intuitive than most and is missing common timeline, map, and graph views. Again, their BPO services can aid customers with full fraud prevention management services. A large number of standard reports are available, and the dashboards can be customized. Call center integration is not offered.

Tietoevry is ISO 27001/9001/22301/14001 and SOC 1 Type 2 certified. They also assert PCI DSS and EU PSD2 compliance. Tietoevry protects its services through per-customer API rate limiting, built-in IaaS services for DoS attack protection, and WAFs that detect and stop protocol-specific attacks while providing API firewall features to identify and respond to abuse effectively. It uses IaaS auto-scaling to meet customer demand. SLAs are negotiable per customer. Initial setup assistance is limited. Documentation is provided in English. Tietoevry manages consent for customers of its banking solutions and through implied

consent via customer relationships, while protecting consumer data using privacy-enhancing technologies like encryption, anonymization, pseudonymization, and aggregation. Data retention policies are automatically set for GDPR compliance.

Tietoevry has excellent functionality in IDV, credential intel, and UBA. It is well suited for banks needing higher levels of identity assurance and AML/KYC and name/watchlist screening. Banks that are card issuers will find the combination of IDV and credit card fraud detection very useful, since not all FRIP providers offer both kinds of capabilities in a single solution. It needs behavioral biometrics to detect bots, however. Although Tietoevry is strongly associated with the Nordic region, their solution is suitable for banks, especially card-issuing banks, in any region.

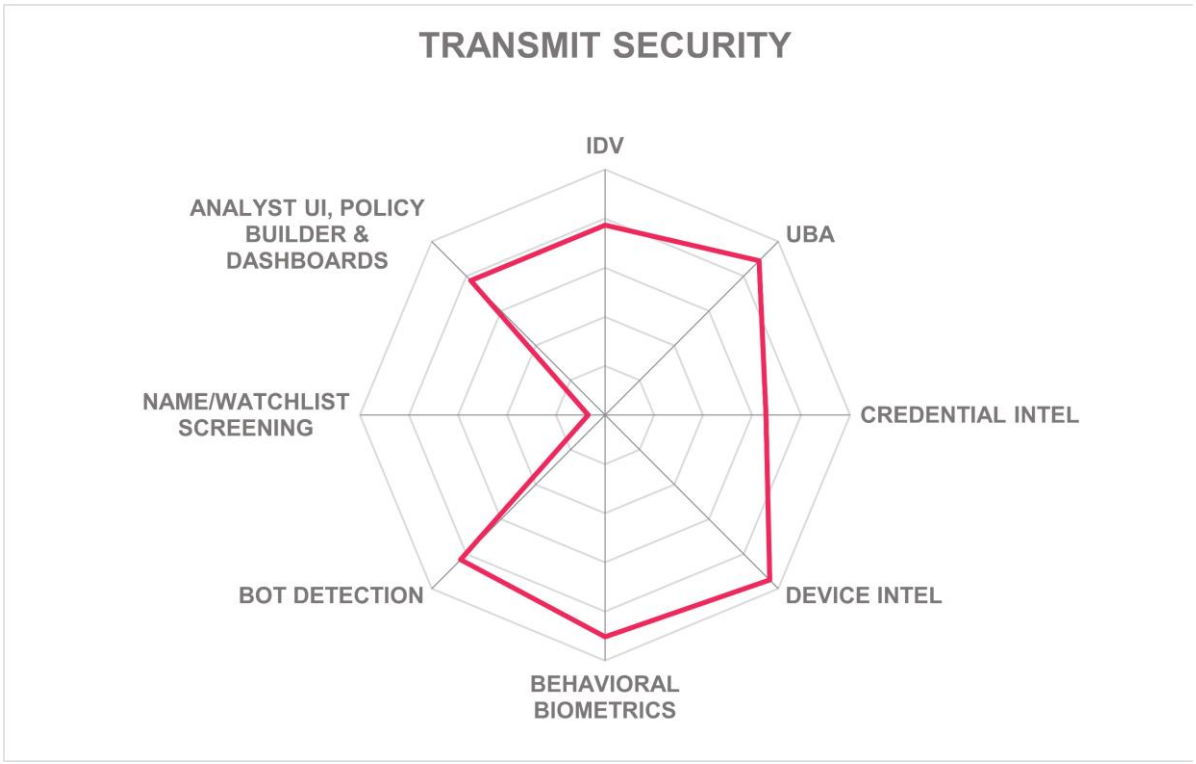
Strengths

- Contains IDV functions; SDK allows for remote onboarding with cutting-edge liveness detection methods.
- Provides AML, KYC, and sanctions/PEP screening.
- Good protection against most types of credit card fraud.
- Addresses mule account discovery, APP and BNPL fraud, and scams.
- Adept at detecting rogue merchants.
- Data storage policies comply with GDPR.
- Built-in case management plus ITSM integrations available.
- Full business process outsourcing and fraud management services offered.
- Many security certifications.

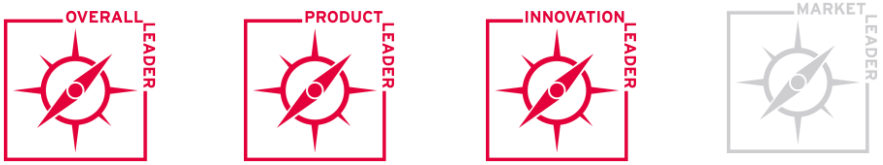
Challenges

- Integrations with more third-party IDV services would enable expansion beyond the Nordic countries.
- Device intelligence should encompass more attributes.
- Lacks behavioral biometrics; bot detection is constrained to UBA since behavioral biometrics are not present.
- Policy authoring is complex, but they have a support team to assist.
- The fraud analyst interface needs to be revamped to improve usability.

Transmit Security – Mosaic Platform



Leader in



Transmit Security was founded in 2016 and is headquartered in Tel Aviv, Israel and Boston, Massachusetts in the US. They are a well-funded late-stage VC-backed company. Their Mosaic Platform contains functionality in most of the FRIP functional areas defined above. Transmit also has leading products in the Passwordless Authentication and CIAM spaces. Transmit Mosaic Platform is a highly scalable SaaS that runs in public IaaS providers across globally distributed datacenters. On-prem and private cloud options are also available. The client portions are JavaScript and mobile SDKs. Pricing is by the on a per API call basis, with bundles available.

Transmit's IDV functions aid customers with KYC and AML in conjunction with third-party services, although it is not designed as a full AML solution. It does not do name/watchlist screening. The risk analysis and authentication services can inform 3DS2 ACS and EU PSD2 SCA and TRA processes.

Transmit can detect all forms of credit card fraud, including CNP, CNR, counterfeit cards, malicious card testing, and protect against transactions from skimmers and chargeback abuse. It detects and prevents mule account activities through a combination of IDV and UBA functions. The platform prevents APP fraud by monitoring suspect user activity (including information from call centers, web, mobile, and in-branch) and chains of compromised accounts to identify potential fraudsters. It deters BNPL fraud by examining identity attributes and user behavior. Their IDV services can flag likely NAF and synthetic identities. Transmit can detect government benefits fraud by identifying synthetic identities or excessive claims through historical analysis. Its UBA implementation addresses crypto/dating/travel scams by analyzing unusual transaction patterns and looking for signs from behavioral biometric analysis that the user is being manipulated.

For IDV, Transmit has a mobile SDK that enables remote onboarding with selfie-to-official ID document matching and innovative liveness detection. It can also orchestrate additional checks to third-party IDV services. It has in-network compromised credential intelligence and can be configured to call external sources by customers. Transmit's SDKs pull the full range of device attributes for evaluation. It conducts device posture checks and can detect jailbroken devices, malware, and SIM swaps. It can also be configured to call out to MNOs for updated, granular location information. Its UBA functions scrutinize a long list of login and transaction details, including transaction types/amounts/payees/items purchased, relationships to known high-risk accounts, multiple attempts from multiple users on a single device, and proximity to suspicious activities. The SDKs and JavaScript provide thorough behavioral biometrics, including the standard and some leading-edge modalities. These capabilities are used to prevent ATOs. Bot detection is driven by a combination of behavioral biometrics and activity signatures. Transmit also has advanced bot management features including allow- and denylisting, challenges, throttling, and redirection.

Transmit makes rule and policy building comparatively easy with a flow-chart style interface and movable sliders for adjusting risk factor weights. It can yield decisions or risk scores with customizable reason codes, and it can package results as JWT claims, SAML assertions, OAuth2 grants, OIDC flows, or HTTP headers. The API types supported are REST, Webhooks, and WebAuthn. Dashboards provide the essential information, and analysts can drill down from there to start investigations. The fraud analyst interface allows administrators to define multiple investigative workflows as templates. Queries can be turned into repeatable reports. Case management features are built-in, and generic connectors facilitate connectivity with ITSMs. Transmit supports call center integration with Genesys, Nuance, and Pindrop, allowing call-to-web session mapping. It can also get call information from MNOs if configured. GenAI is used to create case and event descriptions, executive reports, and to support NL queries.

Transmit has obtained SOC 2 Type 2 certification. They leverage IaaS auto-scaling and have active/active deployments for the highest availability. Customers can choose between

different SLA options. Transmit Security employs third-party security services for detecting request anomalies, uses a layered security model with WAF protection at the edge to detect and mitigate threats, and provides application security controls for monitoring and preventing protocol-specific attacks. The APIs are protected by strong authentication mechanisms. Transmit offers several levels of training and certification for administration and product use, and provides 24/7 global support services, available both on-site and remotely. English, Spanish, and Japanese are supported. As an integrated CIAM vendor, Transmit can collect consent for PII usage, and it protects customer data using de-identification, pseudonymization, redaction, and encryption to adhere to privacy regulations.

Transmit Security has CIAM and FRIP capabilities, and the company is approaching the market with a combined offering. This is advantageous for organizations that are looking to upgrade. Transmit is focused on large organizations in the financial sector. Transmit has good capabilities for IDV, device intel, UBA, and behavioral biometrics. Their ability to detect the different forms of credit card fraud will be of interest to card issuers. Their strong orchestration features allow it to work with other IAM and FRIP components. Banks and issuers should strongly consider Transmit Security's solutions when conducting RFPs.

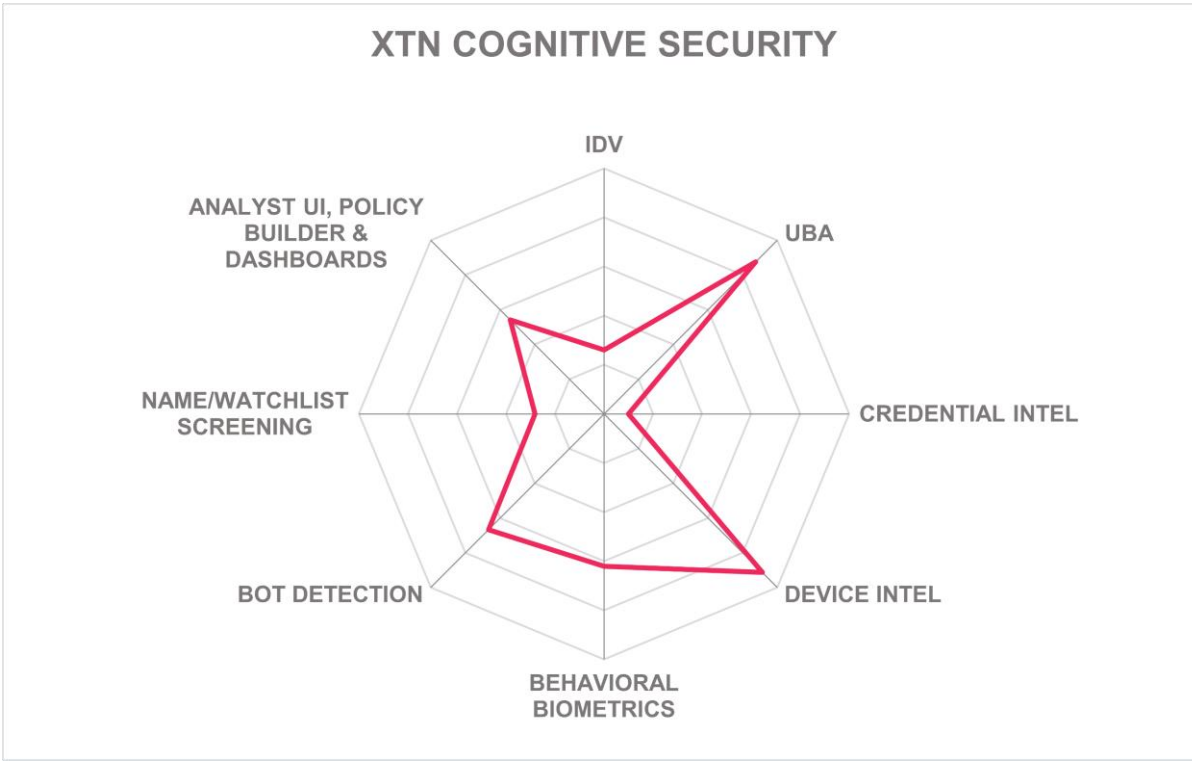
Strengths

- Provides IDV functions, including remote onboarding app with multiple, innovative liveness detection methods.
- Easy to use journey builder facilitates complex orchestration if needed.
- Excellent coverage of credit card fraud detection methods.
- Detects APP and BNPL fraud, NAF, and scams.
- Device intelligence looks at all available parameters.
- Excellent behavioral biometrics for user profiling and bot detection.
- GenAI for case descriptions, executive reports, and natural language queries.

Challenges

- Does not do name/watchlist screening.
- Built-in AML and KYC support could be improved, although AML/KYC can be orchestrated within Transmit Mosaic leveraging third-party services.
- Credit card detection requires partner integrations.
- Language support could be expanded.

XTN COGNITIVE SECURITY® – Cognitive Security



XTN Cognitive Security®, founded in 2014 in Italy, is a privately held company backed by the majority shareholder CY4GATE SPA, listed on the Milan Stock Exchange. Their primary product, the XTN Cognitive Security Platform, is a cybersecurity and fraud prevention tool. XTN covers the device intelligence, UBA, behavioral biometrics, and bot detection parts of FRIP. It is primarily SaaS-delivered, leveraging two IaaS providers and datacenters in Europe. Customers can also choose to run it on premises or in private clouds. The client-side components are JavaScript and SDKs. The majority of XTN's clients are based in the EMEA region, with a focus on Southern Europe, and are primarily in the finance sector. They offer licensing models that charge per user or per analyzed transaction, tailored to specific use cases.

XTN provides an orchestration layer that enables customers to integrate sanctions and PEP list feeds and build custom screening rules based on that data. This enables basic AML compliance, but there are no features for KYC. It does not facilitate SAR filing.

It can look for CNP and counterfeit credit card usage, chargeback abuse, and malicious card testing. To detect mule accounts, it watches account openings and transaction flows. XTN can detect when users are being manipulated over the phone in APP schemes and look for Remote Access Trojans (RATs) or legitimate remote-control software that might be used for nefarious purposes. To deter BNPL fraud, XTN scrutinizes applicant behavior during credit application processes. XTN's behavioral biometrics enables it to detect new account NAF and synthetic identity fraud. It can detect financial scams. For EU PSD2 compliance, XTN centrally manages SCA exemptions, performs risk analysis for Third-Party Providers (TPPs), and assists in preparing the monthly fraud reports required by central authorities. Due to XTN's dual focus on the insurance as well as finance industries, it can discover fake brokers and insurance claim fraud.

The solution does not have built-in IDV functions, but customers can integrate third-party services via the console. It does not use compromised credential intelligence. XTN's JavaScript and SDKs (Android, iOS, Flutter, ReactNative, and Apache Cordova) pick up all the relevant device attributes and perform device posture checks, known user on new device checks, and can discover if devices are jailbroken or contain malware. XTN's UBA functions examine an extensive list of login and transaction details including transaction types/amounts/payees/item analysis/location, proximity to suspicious activities, multiple attempts from multiples users on the same device, relationships to known high-risk accounts, and income-to-spending analysis. XTN's SDKs pick up behavioral biometric signals including most of the basic and a few innovative modalities. The combination of device intel, UBA, and behavioral biometrics enables ATO detection. Behavioral biometrics also forms the basis of their bot detection capabilities. Bot management options include allow- and denylisting and challenging suspected bots.

The granular risk engine returns scores with configurable explanations. Decisions are not provided as customers determine how their applications process the scores. Packaging evaluation results into claims or assertions is not yet supported. XTN includes GenAI in the interface to help configure risk factor weighting. REST and SOAP APIs, Webhooks, and queues are supported. It can integrate with and orchestrate workflows in call center software.

Dashboards are adequate but cannot be personalized by analysts, and they could be redesigned to improve usability. Custom reports can be constructed. The analyst interface has map and timeline views and a link analysis tab that shows how transaction elements are related to other events. Case management is provided in the analyst interface, and there are integrations with JIRA and ServiceNow ITSMs.

XTN is ISO 27001 certified. XTN enforces API rate limiting, has strong authentication options for its API, relies on anti-DDoS protection from cloud services, incorporates input validation and security patch management to prevent protocol-specific attacks, and utilizes API firewall features through their cloud provider to identify and respond to potential abuse. Their SaaS uses standard IaaS auto-scaling to ramp up and down as needed. Setup and incident handling support are provided. Documentation and support are available in English, French, and Italian. Consumer data consent is handled by their customers, but their platform uses privacy preserving technologies like de-identification, pseudonymization, and encryption.

XTN targets the financial sector and serves the use cases of payments/credit card/APP/BNPL fraud detection well with device intelligence, UBA, and behavioral biometrics. They have some functional omissions in IDV and compromised credential intelligence that would make the solution more extensible for banking applications. Banks and fintechs that have satisfactory IDV services as well as credit card issuers should strongly consider XTN, given their deeply granular UBA capabilities.

Strengths

- UBA and transaction analysis functions encompass a wide range of risk factors, including some which are unique to this solution.
- Some coverage of credit card fraud types.
- Uses UBA and behavioral biometrics to stop APP, BNPL fraud, various scam types, and mule accounts.
- Addresses several forms of insurance fraud.
- Good implementation of behavioral biometrics.
- Case management and ITSM integrations available.

Challenges

- Lacks compromised credential intelligence.
- Does not have in-built IDV functions; integrations with third-party services possible but require configuration.
- AML features could be expanded; KYC not present.
- Dashboards need to be reorganized for optimal reporting and investigations.

Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other companies in the market that readers should be aware of. These vendors did not participate in the rating for various reasons but nevertheless offer a significant contribution to the market space.

Amazon

Amazon was founded in 1994 in Seattle, Washington in the US. Amazon Fraud Detector is a service available in AWS for customers that has features for detecting online payments fraud, NAF, trial and loyalty program abuse, and ATO fraud. The solution is highly scalable and leverages ML detection models.

Why worth watching: Amazon hosts many ecommerce applications, providing a potentially large customer base for Amazon Fraud Detector. They also offer a Free Tier with up to 30,000 fraud predictions per month.

Brandefense

Brandefense was founded in 2018 in Turkey. Brandefense monitors cybercrime activities to continually update their understanding of attackers' tactics, techniques, and procedures (TTPs). Brandefense has an emphasis in stolen credit card monitoring, which helps issuers and merchants. Their other solutions include brand protection, external attack surface management, and third-party risk management.

Why worth watching: They look for compromised credentials and identity theft on the dark and deep web.

Deduce

Deduce was established in 2019 in New York, US Deduce supports the FRIP market by offering real-time behavioral intelligence derived from a large-scale identity network that spans hundreds of millions of profiles. It enhances CIAM and FRIP systems by detecting anomalies in login behavior, new device usage, or impossible travel patterns, without requiring PII exchange or browser fingerprinting. Deduce's risk signal enrichment helps inform risk-based authentication flows and fraud analytics platforms, enabling dynamic, step-up challenges or session termination based on inferred trust levels.

Why worth watching: Deduce has an innovative identity graph that expedites investigations. They were just acquired by Cheq in early 2025.

Equifax

Equifax is one the "Big Three" credit rating agencies, and has services across most FRIP categories, including authoritative identity proofing, AML, KYC, and OFAC compliance. They

also offer MFA, risk management, and other related services. They are headquartered in Atlanta, Georgia, US.

Why worth watching: As an authoritative attribute provider, Equifax is part of the fraud protection supply chain. Equifax acquired Kount in 2021 and Midigator in 2022 which gives them additional FRIP functionality.

F5

F5 was founded in 1996 and is a leading network application delivery and security provider headquartered in Seattle. F5's entry in FRIP is largely based on Shape Security's tools which they acquired in 2020. Their Distribute Cloud Data Intelligence product is their FRIP offering. Their products cover credential and device intelligence, UBA, and bot detection & management.

Why worth watching: F5 has a broad customer base covering many financial and ecommerce solutions. They were leaders in the last edition of this report, and we hope to include them in the next edition.

Feedzai

Feedzai is a fraud risk detection and risk operations specialist firm headquartered in Portugal. In 2021, they acquired Revelock, the former Buguroo, another FRIP vendor. Feedzai covers financial fraud use cases, account opening fraud, AML, KYC, and watchlist screening.

Why worth watching: Feedzai recently introduced new GenAI features to help fraud fighters including scam alert descriptions, case summarization, an LLM-based tool for creating SARs, and a natural language rules editor interface.

FICO

FICO is a long-established analytics and risk management company, founded in 1956 in California, US. The FICO Falcon Global Intelligence Network gathers risk signals from more than9,000 global institutions. FICO Falcon Fraud Manager aids in preventing ATO and payment fraud. They also offer AML, KYC, and sanctions screening compliance solutions for customers.

Why worth watching: FICO is a major player in risk management.

Forter

Forter, founded in 2013 and headquartered in New York City in the US, is a late-stage venture-backed fraud prevention specialist. The Forter Trust Platform is a suite composed of modules for improving customer conversions, reducing false declines, detecting policy abuse and adjusting policies, payments security, and ATO prevention. FRIP components present in

the platform include credential intelligence, device intelligence, UBA, and bot detection and management.

Why worth watching: Forter Trust Platform is integrated into some major ecommerce and payment service provider platforms in the US. Their Trust Platform addresses many fraud reduction use cases specific to the ecommerce and payments industries and provides sophisticated remediation capabilities for policy abuse. They appeared in the last edition of this report, and we hope to include them in the next edition.

GBG

GBG, founded in 1989 in the UK, provides fraud protection through advanced identity proofing services that verify individuals using biometric matching, document authentication, and access to authoritative data sources, helping detect and prevent identity-based fraud such as account takeovers and synthetic identity creation. Integrated into CIAM and fraud reduction platforms, GBG's solutions support regulatory compliance and enable high-assurance identity verification for onboarding or high-risk transactions. Their offerings can be embedded via SDKs and APIs into web and mobile applications, making them adaptable across sectors including finance, healthcare, and digital commerce.

Why worth watching: GBG/Acuant has a full AML/KYC/watchlist screening solution. They appeared in the last edition of this report, and we hope to include them in the next edition.

LynxTech

LynxTech was launched in 2023 in Spain. They are still in the early stages but report that they are profitable already. Most customers are in Europe and South America. LynxTech is primarily an orchestration and risk engine. LynxTech has advanced UBA features.

Why worth watching: The founders have 30 years' experience in designing ML models for fraud detection. One of their USPs is that knowledgeable customers can design and import their own ML detection models. This is advantageous for banks that have created and tuned their own detection models for their particular business requirements.

Microblink

Microblink was founded in 2012, and they are headquartered in New York City, US. They also have offices in Croatia and the US. They provide IDV services with document capture and liveness and deepfake detection. Microblink aids with AML and KYC with sanctions, PEP, and adverse media screening. The solution helps prevent NAF and synthetic ID fraud. They also cover CNP fraud detection and chargeback abuse prevention.

Why worth watching: They target not only FIs and fintechs, but also the travel and hospitality, iGaming, automotive, and ecommerce merchants. Their solutions are also OEM'd into other IDV and FRIP solutions.

Nice Actimize

Nice Actimize is a fraud and financial crime detection service provider based in Israel. They were founded in 1999. In 2020, Nice Actimize picked up Guardian Analytics, another FRIP service provider. Nice Actimize focuses on financial fraud, AML, KYC, and account opening protection.

Why worth watching: Nice Actimize has a good trajectory of acquisitions, integrations, and growth.

OneSpan

OneSpan, formerly VASCO, was founded in 1984 and is headquartered in Chicago, Illinois in the US, and has offices in Brussels, Montreal, and Zurich. They have a suite of related products that cover all aspects of FRIP except credential intelligence.

Why worth watching: OneSpan was a leader in all categories in the prior edition of this report, but was unable to participate in this round.

Ravelin

Ravelin was founded in 2014 and is headquartered in London, UK. Their emphasis is on defending against online payments fraud. They also protect against policy abuse, such as refund and sales promotion abuse, and supplier fraud, as well as ATO and bot-perpetrated attacks.

Why worth watching: Ravelin offers traditional ATO prevention and payments security and has specialized services for the ecommerce ecosystem.

Reality Defender

Reality Defender was founded in 2021. They are headquartered in New York City in the US. They provide call center integration (to detect calls with deepfake audio), deepfake image detection, disinformation detection, and LLM-generated text detection. Real-time video deepfake detection is currently in beta.

Why worth watching: with deepfakes proliferating, the ability to detect them is already imperative. It is likely that full service FRIPs will partner with organizations like Reality Defender to add on deepfake detection capabilities.

Seon

SEON was established in 2017 in Hungary. SEON analyzes users' digital footprints, device characteristics, behavioral patterns, and signals from email, phone, and social media data. It uses data enrichment and risk scoring to support transaction evaluation and policy-based

responses, including optional step-up authentication. It is an API-delivered solution and does not require full PII, which aids with privacy regulatory compliance.

Why worth watching: Seon is used in sectors such as fintech and e-commerce, often integrated into CIAM and FRIP workflows to support adaptive risk-based decisions.

Telesign

Telesign was established in 2005 and is based in Los Angeles, California in the US. Telesign provides phone number intelligence, identity verification, MFA, and bot detection for finance, on-demand, rideshare, and gaming customers.

Why worth watching: Telesign is a service provider to several other vendors in the FRIP market and has many built-in capabilities.

Thales

Thales, headquartered in Paris, France, is a global defense and security company. They have extensive offerings in digital identity and cybersecurity, including the offering of high assurance identity credentials. Thales acquired OneWelcome, a leading CIAM vendor, and Imperva, a leading WAF, in the past few years. Imperva brings ATO protection, bot detection and management, and client-side protection features in the FRIP space.

Why worth watching: Thales provides high assurance identity and bot protection for banks and other industries.

TransUnion

TransUnion IDVision is a Fraud Reduction service, which leverages iovation, their Portland, OR based subsidiary launched in 2004. IDVision has FRIP functionality in the areas of ID proofing, device intel, and bot detection.

Why worth watching: TransUnion is one of the “Big Three” credit rating agencies with broad scope for authoritative attributes. TransUnion services are utilized by other FRIP service providers. In 2022, TransUnion acquired Neustar, another large FRIP service provider. TransUnion was covered in the previous edition of this report but was unable to participate in the update.

Related Research

Leadership Compass: Fraud Reduction Intelligence Platforms 2023

Buyer's Compass: Fraud Reduction Intelligence Platforms - Finance

Leadership Compass: Fraud Reduction Intelligence Platforms 2021

Copyright

KuppingerCole Analysts supports IT professionals with exceptional expertise to define IT strategies and make relevant decisions. As a leading analyst firm, KuppingerCole offers firsthand, vendor-neutral information. Our services enable you to make decisions crucial to your business with confidence and security.

Founded in 2004, KuppingerCole is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as technologies enabling Digital Transformation. We assist companies, corporate users, integrators, and software manufacturers to address both tactical and strategic challenges by making better decisions for their business success. Balancing immediate implementation with long-term viability is central to our philosophy.

For further information, please contact clients@kuppingercole.com..