paladin vendor report | **fraud prevention**

2026

TENTH ANNIVERSARY

paladinfraud

The 2026 Paladin Vendor Report

The commerce landscape is increasingly complex. This report cuts to the chase. Every day at Paladin Group, we're in the thick of the fast-paced world of fraud solutions. With dramatic changes coming quickly, including AI "assistants" or "Agents" handling shopping tasks on the customers behalf, commerce and business models are ever-evolving. So it's crucial to remain focused on streamlining and maximizing the capabilities of organizational fraud management operations while reducing checkout friction and preparing technology to identify legitimate agent-led activity without increasing false positives.

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

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

Because of the constant evolution of many popular fraud mitigation solutions, we decided to provide the Paladin Vendor Report (PVR) on an annual basis. And now, we're pleased to publish the latest: the 2025 Paladin Vendor Report. We've offered

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

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

previous participants the chance to update their sections and incorporated additional participating vendors.

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

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

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

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

- User Behavior & Reputation
- 3DS & Consumer Authentication
- Fraud Platforms & Decision Engines
- Identity & Data Verification
- Chargeback Management & Platform

Introduction

Core functionality icon key

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

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

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

AI Powered – Matching algorithms to detect anomalies in the behavior of transactions or users.

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

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

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

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

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

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

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

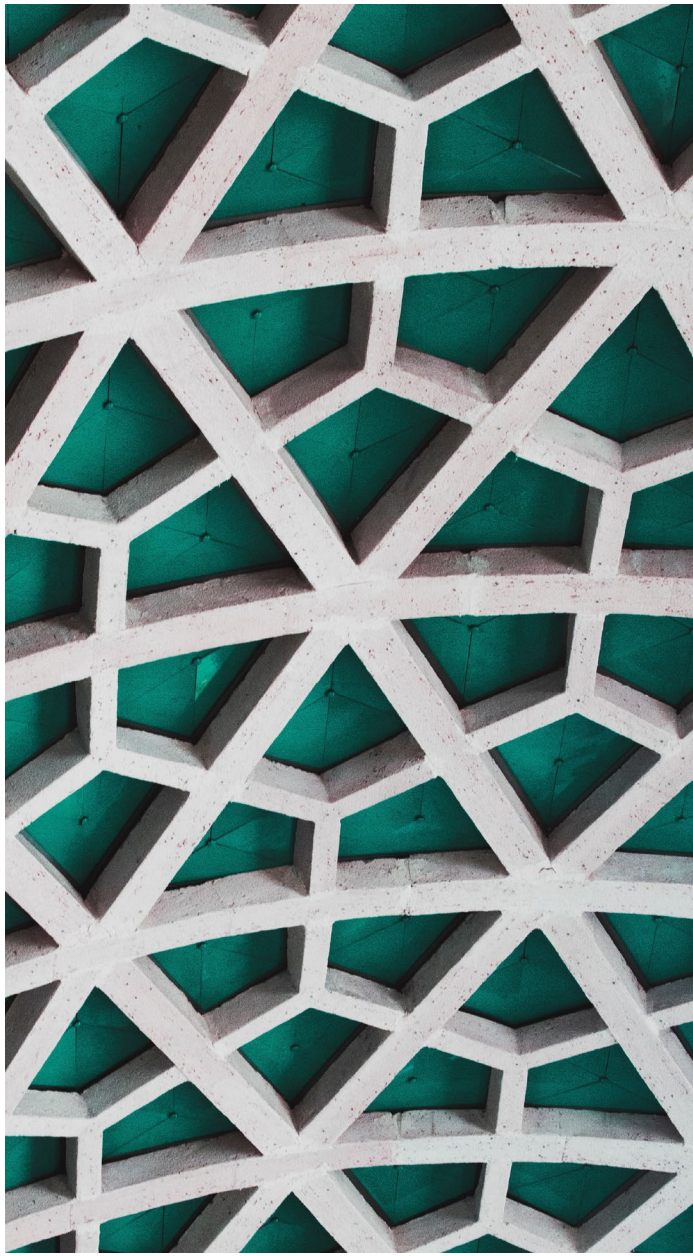
Pre-Authorization Functionality – Ability to score and/or decision a transaction prior to authorization.

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

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

Identification & Data Verification

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



Socure

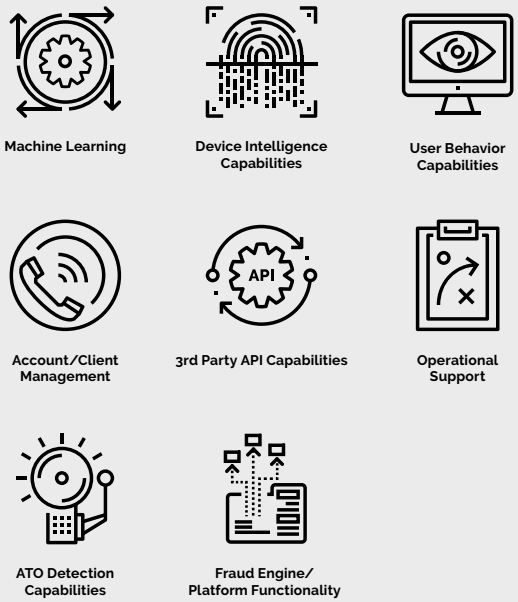
Socure is a leading provider of AI-powered digital identity verification and fraud prevention solutions, trusted by some of the largest enterprises and government agencies to build trust and mitigate risk, anytime through the customer lifecycle. Extensively leveraging AI and machine learning, **Socure's** platform helps users achieve some of the highest accuracy, automation and capture rates in the world. With the acquisition of Effectiv in 2025, **Socure** expanded its capabilities to offer end-to-end identity fraud and payment risk management, integrating advanced transaction monitoring, credit underwriting and know-your-business (KYB) solutions into its platform.

Socure delivers a single, unified platform for identity trust—from stopping identity fraud andmaximizing good customer acceptance at onboarding, to verifying businesses with precision, preventing unauthorized transactions, and optimizing risk-based decisioning, **Socure** uses AI to address emerging threats and restore digital trust.

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

Banks, fintechs, public agencies, marketplaces, gaming, workplaces, and many other verticals rely on **Socure** to deflect attack and scale safely. Socure serves 3,000+ customers, including 18 of the top 20 U.S. banks, 13 of the top 15 credit card issuers, 6 of the top 7 sportsbooks, 600 leading fintechs, the top 2 gig platforms, 4 of the top 5 social media platforms, the top 4 HR information systems, and 132 public organizations, delivering secure, accurate digital identity infrastructure at scale worldwide.

At a Glance:



Socure

Platform Highlights

Unified Identity, Fraud, Compliance, and Risk Decisioning

RiskOS® is **Socure's** unified platform for identity verification, fraud prevention, compliance, and risk decisioning. It consolidates what has historically required multiple vendors and disconnected point solutions into a single platform and API, enabling organizations to make precise, real-time decisions across the entire customer lifecycle, from onboarding and authentication to transactions, account changes, and recovery.

For community financial institutions managing identity, fraud, and compliance with limited technical staff, **RiskOS** can eliminate the operational requirements of integrating and maintaining separate systems for KYC, KYB, AML screening, account takeover prevention, and payment screening. The platform provides a no-code strategy builder that allows risk and compliance teams to configure, test, and deploy decisioning workflows without engineering resources. Pre-built workflow templates developed by industry veterans address common use cases out of the box, and the platform's drag-and-drop canvas enables teams to design and deploy complex decision logic with complete audit history, adapting to new threat vectors in real time without waiting on IT.

RiskOS integrates **Socure's** own AI-powered identity and fraud intelligence with a broad ecosystem of 180+ pre-integrated third-party data services, all accessible through a single API connection. This means institutions gain access to extensive data coverage without procuring, integrating, or managing individual vendor relationships.

Identity Graph and SocureID

Every decision in **RiskOS** is powered by **Socure's** proprietary Identity Graph, the largest in the industry, comprising hundreds of billions of identity elements and 40 billion historical known outcomes. This consortium-driven data asset creates a compounding network effect: the more organizations that contribute outcomes, the more accurate and comprehensive the intelligence becomes for every participant.

Socure's Identity Graph achieves a 96.4% identity recurrence rate, meaning the vast majority of identities presented to the platform have already been seen and verified within the network. With 314 million recurring identities, the platform provides a holistic risk view that includes verified devices, email addresses, phone numbers, transaction history, and behavioral analytics.

SocureID: A Persistent Identity Anchor Across Use Cases.

Each identity that passes through RiskOS is resolved and mapped to a unique **SocureID**, a single persistent identifier that connects every email, phone number, address, device, behavior, KYC result, and watchlist decision into one unified profile within

Socure

Socure's Identity Graph. **SocureID** removes duplicates, preserves historical context, and ensures that every decision made about an identity, whether at onboarding, login, payment screening, or account recovery, draws from the same resolved source of truth. For community financial institutions, **SocureID** eliminates the fragmentation that occurs when different systems maintain disconnected views of the same customer, creating a single thread of identity intelligence that spans the entire member or customer relationship.

Proactive Risk Notifications. Because **SocureID** maintains a persistent, continuously updated profile for each resolved identity, RiskOS enables organizations to receive proactive alerts when the risk profile of an individual changes over time. Rather than relying solely on point-in-time checks at onboarding or login, institutions are automatically notified when identity attributes shift, new fraud signals emerge, sanctions or watchlist exposure changes, or consortium-level risk patterns are detected. This shifts risk management from a reactive posture, where threats are only caught when a customer initiates an action, to a proactive model where the institution is alerted to emerging risks before they result in losses. For community financial institutions with limited fraud investigation staff, proactive notifications ensure that high-priority risks surface automatically rather than depending on manual portfolio reviews or periodic batch screening.

Multi-Tiered Graph Intelligence: Local and Global

Socure's graph strategy operates at two tiers, each delivering distinct value:

Global Graph. The Global Graph is **Socure's** cross-industry consortium intelligence layer, built on hundreds of billions of identity elements and 40 billion known outcomes from 3,000+ customers. It powers **Socure's** AI models and risk scores by providing cross-institution visibility into fraud rings, velocity anomalies, synthetic identity patterns, and first-party fraud behavior. Community financial institutions benefit from the same consortium intelligence that protects 18 of the top 20 U.S. banks and over 600 fintechs. Fraud patterns identified at the largest institutions immediately strengthen protections for every customer on the platform, without smaller institutions needing to build or maintain proprietary data assets of their own.

Local Graph. Local Graph is an enterprise-specific intelligence layer within **RiskOS** that connects every identity to its activities and risk signals across an organization's own ecosystem in a single, time-aware framework. Where the Global Graph provides cross-industry intelligence, Local Graph gives fraud, risk, and trust teams the ability to see how an identity appears today, how it has behaved historically within their institution, and how individual identity elements such as devices, phone numbers, emails, and IP addresses relate to one

another over time. Local Graph is supported by two capabilities:

1. **Persistent Profiles** provide a dynamic, always-on view of how any identity element interacts with an organization over time. Profiles unify every known interaction, signal, and linkage, eliminating blind spots and giving analysts a complete understanding of historical context in a single place.
2. **Connected Rule Writing** allows organizations to build decisioning rules using historical activity, relationships, and velocity patterns rather than relying solely on point-in-time data. Teams can incorporate behavior from earlier touchpoints, including account opening, password resets, logins, transactions, and disputes, into automated decisions.

Together, the Global Graph and Local Graph give community financial institutions two layers of fraud intelligence that would be impossible to replicate independently: the collective knowledge of the industry's largest consortium, combined with institution-specific behavioral patterns that surface risks unique to their own portfolio and member base.

AI-Native Platform with Embedded Intelligence

RiskOS embeds AI throughout the platform, not as an add-on feature but as core infrastructure. The **RiskOS** AI Suite, launched in late 2025, includes six purpose-built AI agents and assistants that automate and accelerate key tasks across the risk lifecycle. A rule writing assistant enables compliance and fraud teams to create executable decisioning rules in plain language through a no-code interface. A case review assistant suggests case outcomes based on scores, signals, and user history, reducing manual review time and improving consistency. A business intelligence agent automates KYB due diligence by scanning a company's full public web presence, ownership structure, and adverse mentions, cutting 30+ minutes per review. GenAI-powered explainability provides one-click, plain-language explanations of model scores and workflow decisions, strengthening audit trails and supporting regulatory transparency.

These capabilities directly address a persistent challenge for community institutions: maintaining effective fraud and compliance operations with small teams. By automating rule creation, case triage, and decision documentation, RiskOS reduces the specialist headcount required to operate a sophisticated risk program.

Primary Use Cases for Community Financial Institutions

RiskOS supports end-to-end fraud, risk, and compliance operations through pre-built, configurable use cases designed for the needs of community banks and credit unions:

Consumer Onboarding. Integrates identity verification, fraud risk scoring, KYC, and compliance screening into a single workflow. As a leading platform, it achieves approximately 90% automated approval rate while minimizing fraud and friction. Advanced Pre-Fill capability

verifies identities with just two pieces of PII and an authentication method, reducing application abandonment and accelerating time to account opening.

Business Onboarding (KYB). Automates Know Your Business verification, Ultimate Beneficial Owner (UBO) checks, and entity risk assessment. Platform integrations with partners like Middesk and Markaaz deliver comprehensive business intelligence, cutting 30+ minutes per manual review and reducing the operational burden of commercial account onboarding.

Login and Account Takeover Prevention. Provides real-time authentication and risk-based step-up verification triggered by device, behavioral, and identity signals. The platform detects and blocks unauthorized access attempts, including those driven by GenAI-powered spoofing of emails, phone numbers, and geolocations, while minimizing friction for legitimate users during login, password resets, and account recovery.

Bank Account Verification. Validates account ownership and status in real time, supporting secure account funding, direct deposits, loan payments, and transfers. The solution proactively prevents unauthorized transactions and reduces fraud risk in money movement. Coverage has recently expanded to 30+ countries for institutions with cross-border needs.

Workforce Verification. Confirms that job applicants are real, legitimate individuals at the start of the hiring process by validating identity, device, and behavioral signals against authoritative data. Blocks over 70% of fraudulent applicants before they reach recruiters. For employees, it extends verification into ongoing access to systems, data, and payroll through persistent identity checks, sanctions and watchlist screening, and risk-based step-up verification. **SocureID** ties applicant screening and ongoing employee checks to the same resolved identity, ensuring consistent and auditable risk evaluations from hiring through access and payroll.

Payment Screening. Provides sanctions screening and watchlist monitoring to support BSA/AML compliance obligations. Socure's Global Watchlist Screening with Monitoring uses an AI-driven, two-stage matching approach that improves match precision and lowers false positives compared to legacy solutions, reducing manual review effort and strengthening auditability.

Socure's Product Highlights

Sigma Identity Fraud is **Socure's** market-leading solution for detecting and preventing third-party identity fraud at onboarding and across the customer lifecycle, delivering a holistic, AI-driven approach by analyzing every identity element in real time.

It uniquely combines personally identifiable information (name, email, phone, address, date of birth, SSN) with digital signals

including device intelligence, behavioral analytics, IP address, geolocation, relationship data, and historical transactional patterns from **Socure's** Identity Graph, powered by billions of outcomes from 3,000+ customers across 20+ markets. By assessing these patterns across institutions, geographies, and timeframes, Sigma Identity Fraud detects anomalies that signal identity theft or manipulation at the entity level, achieving up to 89% fraud capture in the riskiest 5% of applicants and up to 85% in the riskiest 3%—more than double the industry average—while reducing false positives by over 40% and driving manual review rates below 5%.

Sigma Synthetic Fraud is Socure's market-leading solution for detecting and preventing synthetic identity fraud in real time. Purpose-built to address its unique and evolving nuances, this AI-driven model leverages synthetic-specific features to identify even the most sophisticated fabricated and manipulated identities in real time.

The result is best-in-market performance, capturing up to 83% of synthetic fraud within the riskiest 5% of applicants, enabling institutions to stop synthetic identities at the door while preserving seamless approval experiences for legitimate users, including hard-to-verify and thin-file populations.

Sigma First-Party Fraud is a consortium-based solution that stops bad actors at scale by providing visibility into their activity across the broader financial ecosystem. As the largest cross-industry first-party fraud consortium, it brings together a uniquely diverse network of organizations across financial services, fintech, online gaming, BNPLs, payment apps, credit unions, marketplaces, and more. In 2025 the consortium achieved significant scale, amassing data intelligence encompassing 416+ million identities, 20+ billion transactions, and 520+ million accounts.

Sigma First-Party Fraud is the only holistic first-party fraud solution that delivers two predictive risk scores — Identity Manipulation Score and Dispute Abuse Score — as well as real-time, actionable intelligence to help detect repeat abusers and predict the risk that a true identity will act in bad faith. This proactive approach helps organizations drastically reduce losses, cut operational costs, and build a trusted ecosystem for good users.

Backed by the largest cross-industry consortium, Sigma First-Party Fraud analyzes risk signals — such as dispute patterns, payment denials, and account closures — to uncover individuals who manipulate their identities or financial behavior for bad-faith activities. These real-time insights, combined with the two aforementioned risk scores, quantify the likelihood of an individual engaging in first-party fraud after account opening. Additionally, real-time alerts enable organizations to take immediate action, preventing repeat fraud and minimizing risk exposure.

Socure

Email, Phone, and Address RiskScores verify the trustworthiness and ownership of a phone, email, or address to enhance fraud and scam detection across the customer lifecycle. These machine-learning models evaluate newly presented PII to distinguish legitimate users from sophisticated threats with minimal user input.

Email RiskScore assesses the risk of a name/email pair in real time by verifying the correlation of these elements and evaluating hundreds of good-versus-risky signals, including indicators of fake, machine-generated, invalid, high-velocity, and low-tenure email usage associated with that identity. It performs real-time anomaly detection at the individual, company, industry, and network level to uncover unusual identity–PII linkages and risky behavior patterns, while leveraging consortium and authoritative data to distinguish trustworthy from suspicious associations. Additionally, Email RiskScore measures how often an email has been linked to an identity, as well as the frequency of risky or trustworthy outcomes tied to that pairing, to drive more accurate decisions.

Phone RiskScore confirms name/phone ownership and assesses the risk associated with phone numbers to enable proactive fraud prevention with enhanced confidence and accuracy. The solution analyzes phone-specific intelligence such as line type and tenure, carrier information, and identity–PII velocity, and checks against Socure's proprietary positive and negative phone data and broader network identity graph. It also performs real-time anomaly detection and SIM swap detection to flag high-risk changes or usage patterns that could signal account takeover or other forms of fraud.

Address RiskScore helps prevent malicious actors from hijacking or creating accounts with compromised or synthetic physical addresses by verifying the validity of a given address and determining the strength of association between the address and the identity. The solution analyzes a wide range of address-related signals such as delivery and mail activity patterns and the characteristics of P.O. boxes, commercial locations, military addresses, correctional facilities, and more, enabling incredibly broad and accurate address verification.

Digital Intelligence Suite delivers real-time, actionable risk and trust signals across the entire digital journey—from onboarding and login to high-risk transactions and contact center flows.

Bringing together three core services in real-time in 200ms — Device Intelligence (device-level across 900M device signals per month and network risk signals), Behavioral Analytics (session-based behavior analysis), and Entity Profiler (PII-to-device linkage and digital presence)—the suite binds each identity to its devices, behaviors, and historical interactions to continuously detect anomalies and prevent account takeover and abuse.

Powered by hundreds of device, behavioral, and network signals, Digital Intelligence forms a single, comprehensive risk layer that

feeds directly into Socure's AI models listed above—such as Sigma Identity Fraud, Sigma Synthetic, First-Party Fraud, and Predictive

DocV—and is fully orchestrated through the RiskOS decisioning platform. This enables a true, comprehensive view of identity—going beyond confirming a customer is who they claim to be to also determine whether they are a real person and whether it's safe to do business with them. Persistent identity decisioning provides a dynamic "digital signature" for each user, giving organizations a unified, cross-session view of risk.

Socure's Compliance Suite provides seamless, automated compliance across the entire customer journey. It's delivered via a single API and unifies customer verification, sanctions screening, ongoing monitoring, and decisioning into one orchestrated Workflow—offering extensive data coverage, precision, accuracy, and controls that can help stand up to regulatory scrutiny.

Socure Verify delivers accuracy, reasoning, address verification, and risk alignment for Customer Identification Program (CIP) and KYC verification. Powered by AI and machine learning, Socure's triangulated data approach can help verify identities across multiple trusted sources to support CIP and KYC requirements, correlating thousands of online and offline identity signals to resolve to the single best matched entity. This methodology enhances fraud detection, reduces false positives, and can support compliance while enabling seamless onboarding for all demographics, including hard to identify populations.

Socure achieves verification rates of up to 99% for mainstream populations and industry-leading, high-90s verification rates for Gen Z and other thin-file or new-to-country applicants. With considerable Gen Z coverage, **Socure** verifies 70% of 18-year-olds opening their first financial accounts—30% more than legacy providers—and delivers verification rates in the mid-90s for 18- to 25-year-olds. Additionally, **Socure** delivers high verification rates for 13- to 17-year-olds. Available in over 190 countries, **Socure's** proprietary models and verification techniques, can support precise identity matching even in cases of name variations, nicknames, misspellings, or reordered name structures.

Electronic Consent-Based Social Security Number Verification (eCBSV) provides an additional identity verification layer to combat synthetic identity fraud and enhance CIP compliance. By directly matching an individual's name, Social Security Number (SSN), and date of birth (DOB) with the issuing authority, eCBSV enables businesses to make confident decisions, especially for higher-risk consumers, while delivering a 6–8% average additional approval lift for hard-to-identify, thin-file populations such as Gen Z, new-to-country, and other underserved consumers. By using this service, businesses can strengthen fraud prevention, enhance regulatory compliance, and expand access to previously hard-to-verify

Socure

individuals, ensuring more accurate and efficient identity verification.

Socure's Global Watchlist Screening with Monitoring enhances compliance operations with advanced AI and ML, delivering sanctions matching accuracy and scale. A two-stage scoring system—combining name matching with advanced entity resolution and profile matching—helps provide certainty that the individual in question is the correct match, while minimizing false negatives and unnecessary alerts.

By integrating intelligent risk assessment, continuous status monitoring, and streamlined case management, **Socure's** solution is 20% more accurate than competing approaches, reduces false positives by 30%, and drives a 75% reduction in manual reviews. Analysts gain a single, workspace to view side-by-side comparisons, prioritize critical cases, and capture reviewable context for audits, supported by daily sanctions, PEP, and adverse media updates. With tiers of global coverage and configurable match parameters, Socure empowers teams to maintain compliance, reduce operational burden, and focus on truly high-risk entities.

Socure's Predictive DocV (DocV) solution verifies a consumer's government-issued identity document against their facial biometrics using advanced document forensics and machine learning–driven decisioning. It is built to handle high volumes of stolen identities, spoofing, and highly sophisticated deepfake and injection attacks that are increasing in complexity.

Socure's proprietary solution addresses multiple attack vectors using a layered approach to protect against fraud, with no impact on the user experience. This strategy analyzes a rich set of document signals in real time, with a broader view of identity risk by also analyzing PII, barcode data, device and behavioral intelligence, geolocation, and biometric signals. Advanced deepfake and injection detection models can analyze camera integrity, device continuity, as well as GAN and diffusion artifacts to distinguish authentic user captures from synthetic or manipulated content. DocV evaluates frame-by-frame motion, liveness signals, and cross-session consistency detect sophisticated injection attacks. All signals can support high rates of accuracy with 98.7% fraudulent attempts detected and a 98%+ automated decision rate.

In addition, **Socure's** user-centric DocV solution includes accessibility features for visually impaired users and supports WCAG 2.1 AA standards, addressing consumer concerns often presented by typical document and biometric verification solutions.

Socure's DocV delivers verification responses in under one second, compared to the industry average of more than 30 seconds.

Socure Account Intelligence provides real-time verification of bank account status andownership across financial institutions, fintechs, credit unions, neobanks, alternative payment platforms, and more.

Socure

With coverage up to 98% bank account status and up to 82% bank account ownership coverage — it enables businesses to verify bank accounts in two seconds or less using only a name, account number, and routing number.

Beyond verification, **Socure** leverages cross-industry intelligence and first-party fraud signals to identify repeat bad actors who use their own bank accounts to exploit systems before transactions can occur.

For more information, visit www.socure.com

paladinfraud

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

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