transmit security

USE CASE

Account Opening

The goals & challenges of account opening

Account opening (AO), done right, welcomes new customers with a quick and easy enrollment flow. Unfortunately, bad actors abuse the same process to open fraudulent accounts and use evasive techniques to fly under the radar. Companies struggle to keep up with their evolving tactics plus ever-changing compliance mandates, like Know Your Customer (KYC) and General Data Protection Regulation (GDPR). Too often, in a race to comply and patch security, companies add more friction than customers will tolerate.

When opening a bank account, for example, customers may be asked to fill out lengthy forms, present a photo ID, set up authentication, answer security questions and enter a one-time passcode (OTP) to prove they truly possess the email or phone number they've provided. Painstaking processes lead 51% of customers to drop off before completing enrollment. What's worse, these security measures don't do enough to prevent AO fraud.

Exacerbating matters, most enterprises stitch together AO products from multiple vendors. They combine fraud detection, authentication, background checks, identity verification and other tools that were not made to work together. Difficult integrations require lengthy development cycles, only to create complexity, silos and disjointed user experiences (UX). Companies are left with vulnerabilities, higher costs and lower revenue.

This paper covers the challenges of account opening, and how Transmit Security solves these issues with a unified, plug-and-play AO platform. Made for enterprises with the most complex infrastructures in the world, our solution delivers the UX and IT simplicity, agility, speed and accuracy to stop AO fraud, ensure compliance and optimize completion rates.

How a unified solution solves these challenges

By design, a unified account opening platform tightens security, simplifies compliance and streamlines the customer experience. Centralized identity management and orchestration make it easy to create seamless AO journeys — from registering, credentialing and verifying customers to validating data and running background checks.

Throughout the AO process, automated fraud detection mitigates risk or elevates trust in real time, based on your company's security and compliance requirements. A modern AO solution leverages AI-driven intelligence to spot risk, even high-quality fake IDs made with 'real' but stolen data. With a consolidated platform, you'll prevent fraudulent accounts, ensure compliance and give customers a quick and easy AO process from start to finish.

Challenges of account opening

Trying to satisfy your account opening use case by piecing together the AO puzzle with disparate solutions leads to account fraud, compliance fines and customer attrition. It's a lot to handle in the face of many challenges:

AO fraud slips past 5+ layers of protection: Bad actors create synthetic identities by combining stolen identity data with a phone number or email account they control in order to: **1** pass data validation; and **2** authenticate with OTPs or email magic links. As 'proof' of synthetic identities, they use high-quality fake IDs, easily purchased or created online to: **3** deceive automated identity verification and manual screenings. Fueling the problem, registration bots are designed to: **4** evade bot detection; and **5** bypass anti-fraud tools by mimicking human behavior, solving CAPTCHA, rotating IPs, spoofing devices and more.

AO fraud evades 5 layers of protection:

01 **Data validation -** by using enough 'real' but stolen data

02 **MFA with OTPs -** by using a phone or email they control

03 **Identity verification -** by using high-quality fake IDs

04 **Bot detection -** by emulating human behavior, solving CAPTCHA, etc.

05 **Fraud protection -** by spoofing devices & human behavior, rotating IPs, etc.

Fraudsters take advantage of multiple point solutions that offer a narrow set of protections, unable to see the full context of all activity. They also evolve their fraud tactics to stay ahead of static or slow-to-adapt defenses. With fraudulent accounts, they open new lines of credit, secure loans, make illegitimate purchases, launder money and commit other crimes. According to a Javelin report, $7B was lost to AO fraud in 2021.

The workload multiplies as security gaps widen: Today's sophisticated, rapidly-evolving AO fraud requires multiple detection methods and data correlation across hundreds of telemetry streams. But attempting to pinpoint suspicious activity with disparate, multi-vendor solutions requires complex integrations, decision-making structures, coding and tuning cycles. Even then, teams of data analysts must standardize risk scores, which can still result in errors, especially if black box AI models are at play.

Operational costs escalate: Companies pay a heavy price in terms of IT overhead, fraud losses and customer attrition:

- In addition to complex integrations, coding and tuning cycles, costs continue to rise as developers struggle to build and maintain layers of heuristic rules to address new or evolving fraud MOs.
- When managing automated identity verification, registration, authentication and other friction-prone aspects of account opening, you must continually monitor and improve the user experience (UX) to minimize drop-offs, a more time-consuming process when dealing with multi-vendor point solutions.
- Likewise, manual processing of identity verification, data validation and background checks, is slow, costly and unable to scale. Moreover, the human eye is simply no match for today's fake IDs made with image editing tools or generative AI.

Compliance mandates add complexity & friction: Keeping up with ever-changing global and regional requirements while continuously monitoring for suspicious activity can be difficult.

- **AML, PEP & KYC:** Financial institutions must comply with Anti-Money Laundering (AML), Politically Exposed Persons (PEP) and KYC regulations, which mandate identity verification with a photo ID, background checks and more. Failure to comply results in penalties and brand damage. Reports show AML fines grew over 50% in 2022, reaching nearly $5B.
- **Privacy requirements:** Companies must also meet data privacy mandates, like the California Privacy Rights Act (CPRA) and GDPR, considered the world's toughest privacy law with fines up to 4% of a company's annual revenue. GDPR specifies requirements for how personally identifiable information (PII) is collected, stored, accessed, modified, transported, secured and erased. Currently, an estimated 70% of EU companies and 90% of US companies are out of compliance with GDPR. At the same time, we're facing new privacy concerns related to generative AI.

  Adhering to privacy requirements is especially difficult when PII is stored across multiple systems. Weak application security and a lack of protection at the data layer leaves PII vulnerable to breach. The root of the problem is twofold: 1) disparate solutions lead to data silos and data sprawl; 2) most CIAM vendors lack expertise in cybersecurity data protection.

Added friction degrades UX and erodes revenue: Long onboarding processes and excessive forms are proven to increase customer drop-off rates. Likewise, asking customers to submit a selfie and photo ID for identity verification may require more time and effort than some customers are willing to invest. AO solutions that lack user-friendly digital interfaces add to the customer's frustration.

To reduce customer attrition, UX teams must continually analyze drop-off patterns and address pain points based on data-driven insights. Static solutions that are difficult to alter, hindering your ability to make improvements that would increase conversions. And without unified visibility and analytics to evaluate and optimize AO completion rates, outcomes are suboptimal.

Account Opening with Transmit Security

Transmit Security is the only vendor to provide a unified AO platform with a full set of native capabilities — designed to address the complete use case out of the box. With a consolidated, end-to-end solution, you can simplify and secure every step of account opening with minimal effort.

Powerful orchestration: Our orchestrated, holistic platform seals the cracks to prevent AO fraud, even deceptive attacks that use device emulators, registration bots, automation frameworks and deepfakes created with generative AI. Orchestration is the lynchpin that pulls all AO capabilities together, providing:

- **Accurate risk scores:** A powerful orchestration engine aggregates and correlates data across AO capabilities, apps and channels to view the full context of risk signals and pinpoint suspicious activity. The results: highly accurate risk scores, delivered instantly.
- **Out-of-the-box decisioning rules:** Once anomalies have been detected, real-time action triggers automatically adapt the AO journey in real time. Pre-made and customizable decisioning rules eliminate the cost and complexity of building and maintaining that decision logic. Our platform lets you call any number of services, data sources and APIs to orchestrate actions based on a holistic view of risk and trust.
- **Drag-and-drop journey builder:** A visual no-code journey editor makes it easy to build and maintain orchestrated account opening flows that optimize security and UX. Simply drag and drop elements into place to design customer journeys, establishing if and when you need identity verification and/or passive data validation, for example.

  Later, without making any code changes to your app, you can easily modify and improve the UX by changing the order of AO steps, for example. You can alter the entire user flow with minimal effort and can even invoke capabilities across channels, enabling advanced onboarding combinations.
- **Cost savings:** Altering the sequence can also enable you to significantly reduce costs. For instance, authenticating the user with an SMS OTP before invoking identity verification would stop fraudsters before they reach verification if they are using a blacklisted phone number or provided a fake or stolen number.
- **Service integration layer:** Our plug-and-play architecture eliminates the need for integrations — no coding required. The platform is modular by design so you can select the account opening capabilities you need.

Intelligent fraud detection: Improves detection of AO fraud, reducing false positives/false negatives by 90% when tested against other solutions. Based on risk scores, your risk tolerance and compliance requirements, our platform can provide recommendations to ALLOW/CHALLENGE/DENY at any point during the account opening process. End-to-end AO fraud protection includes three core components:

- **Multi-method detection:** Examines hundreds of signals to ensure the most accurate detection, based on advanced behavioral biometrics, privacy-age device fingerprinting, bot detection, application and network evaluation, authentication analysis, transaction signing, fraud ring blacklists and other detections, which passively run in the background at all times.
- **Machine learning and AI:** Continually analyzes the full context of all that's happening in real time across the AO process. ML and AI evaluate data in light of known or suspected fraud patterns, bot behavior and the customer's typical behavior, devices and IP addresses as well as the use case and application flows. All anomalies, even subtle deviations, are weighed as part of a holistic, contextual analysis processed by our orchestration engine.
- **Immediate threat response:** To identify new, zero-day attack patterns, ML and AI proactively analyze a broader range of signals. In parallel, Transmit Security threat researchers continually add new detection mechanisms and tune algorithms. In response to a high risk score, you can deny the user from opening an account or challenge them with identity verification and/or passwordless multi-factor authentication (MFA).

Natively-built identity proofing: Automates compliance with AML, PEP and KYC, giving financial institutions AI-driven identity verification that determines if the individual and their photo ID are legitimate with the highest level of confidence. Automated document and selfie analysis catch high-quality fake IDs by leveraging the most advanced capabilities:

- **Deep document inspection:** Examines every detail to discern if the ID is authentic and unaltered, matching dates with templates, fonts, holograms and dozens of other security features. It uses 150+ weighted analyses and ML algorithms to spot fakes.
- **Biometric matching:** Compares the user's selfie and ID photo to verify the person in the document is the same individual who is trying to enroll.
- **Liveness detection:** Ensures the person in the selfie is a live person, not a video or photo and is sensitive enough for micro-movements like blinking.
- **Global coverage:** Supports 10,000+ government-issued photo IDs and is kept up to date, a never-ending project that companies cannot do on their own.
- **Up-to-date threat detection:** As with fraud detection, our researchers analyze new fake IDs and apply their findings, immediately updating ML and AI algorithms.
- **Native identity decisioning:** Enables you to create and orchestrate validation flows and rules to automate decisioning — without any coding.
- **Easy UX:** Our UI provides clear instructions in a simple 3-step process to snap a selfie and both sides of the photo ID. Visual guides and automated messages ensure the customer captures suitable images.

Data validation & background checks: Prevents AO fraud and ensures compliance by assessing the validity of users' data and background when they enroll. It's automated and instant to simplify and expedite customer onboarding.

- **Global and regional coverage:** Aggregated data sources save you from having to vet, integrate and maintain hundreds of data validation sources.

- **Instant background checks:** Scan AML and PEP watchlists, credit bureaus and anything needed for KYC compliance beyond identity verification.
- **Pre-built and customizable:** Allows you to select sources to ensure the name, address, email, phone, DoB and SSN are valid and strongly associated with the user.
- **Passive validation:** Runs in the background without asking customers to take any extra steps that add friction and lead to drop-offs.
- **Device intelligence:** Checks the geolocation and reputation of a mobile device phone to ensure it aligns with the claimed address and phone number.
- **Simultaneous validation:** Performs data checks and knowledge-based authentication at the same time for the sake of speed and aggregation.
- **Data correlation:** Reconciles discrepancies from different sources. Runtime rules processes the results, delivering decisions directly to your apps.
- **Platform synergies:** Unless you're bound to KYC compliance, data validation may satisfy your risk tolerance with the majority of legitimate customers. In the event data validation returns mixed or negative results, orchestration can invoke identity verification to give the user another chance to prove their identity. At the same time, fraud detection provides risk scores, which are weighed in the holistic, contextual analysis of risk and trust.

Phishing-resistant authentication: True passwordless MFA with Transmit Security makes it easy for customers to set up the most secure form of authentication. The credentialing process is automated, much like setting up fingerprint or facial biometrics to unlock a mobile phone. There's no need to create a username and password; once enrolled, the customer never needs to use a password again. It's 100% password free.

- **Passkey support:** Customers simply enroll by generating or choosing their passkey. Depending on your security requirements, this could be a string of characters, a set of symbols or biometric data. Transmit Security offers an added passkey security layer that ensures passkeys only sync across devices and ecosystems with a deliberate transfer of trust.
- **Device fingerprinting and behavioral biometrics:** Perform passive authentication to maintain a high level of assurance throughout the account opening process without interfering with the customer experience.
- **All-in-one authentication:** For optimal cost-efficiency and flexibility, Transmit Security provides a complete set of authentication methods, giving you the option to use passkeys, passwordless MFA, SMS OTPs, email magic links, social logins and passwords. Having all authentication methods in one AO solution ensures a seamless UX while minimizing IT complexity and costs.
- **Adaptive levels of risk and trust:** In moments of risk, you can achieve a higher level of assurance by authenticating customers with fingerprint or face ID. When passwords are at play, you can reduce the level of trust extended to the customer.

Identity management: A single, centrally-managed AO solution optimizes visibility and control across the entire account opening journey. With a unified user store, you gain a single source of truth that aggregates and secures user profiles, including information about each user's authenticators, behaviors, devices, IP addresses and more.

AI-powered identity analytics: With the power of generative AI and large language models (LLMs), we've integrated conversational analytics into our platform. Much like ChatGPT, you can ask text questions and receive answers, giving you instant visibility and insights about your fraud detection data, end users and their security posture. With the ability to view all risk and trust events, you can quickly and easily tune rules to improve security and UX throughout the AO process.

- **Custom graphs and charts:** Our conversational analytics tool also allows you to create personalized visuals on demand. With it, you can ask for any type of chart or graph to gain insights into your apps, users, devices, risk scores, attack types and more. The model delivers a visualization in seconds, enabling you to optimize security and UX.
- **Full platform synergies:** All capabilities within our AO platform benefit from instant access to unified user profiles with risk scores, threat intelligence and other data. Holistic, contextual information further strengthens behavioral biometrics, device fingerprinting, anomaly detection and other AO capabilities managed via one console.

Out-of-the box compliance: Not only does our AO platform comply with AML, PEP and KYC, as described above, Transmit Security ensures data privacy at all times. As a cybersecurity company with expertise in data protection, we've built the most secure AO platform to protect PII. We also maintain those protections to evolve quickly as GDPR, CPRA and other privacy regulations change.

Our platform is architected from the ground up to ensure PII remains secure:

- **Data security:** Transmit Security's deeply embedded data security layer shields data, keeps PII encrypted in every state, limits authorized access, offers tamper-evident logging, active and passive alerts and more.
- **Unified customer profiles:** Our platform consolidates user data from across all channels and apps into a single user store. By eliminating identity silos and data sprawl, we've solved a key problem, making it easier to meet GDPR compliance.
- **Least-privilege access:** Across our AO platform we restrict and control data access with strong authentication. PII, including biometric data, is not accessible to humans.
- **Per tenant encryption:** Data is encrypted with a unique key per tenant, which makes the data much harder to use in the event of a data breach.
- **Custom data retention:** Restricts data retention to the minimum necessary timeframe while still providing the flexibility to accommodate different workflows that require tighter or less restrictive data handling.

- **Avoidance of PII for model training:** This ensures that the large datasets needed to train and evaluate ML models do not compromise data privacy and security.
- **User consent and control:** Has all of the right tools in place for customers to provide consent, correct data inaccuracies and opt out with 'the right to be forgotten.'
- **Audit trails:** Keeping a log or trail of who accessed which records, when, and why, is essential for GDPR compliance.

User-friendly UI: Simple graphic illustrations optimize our guided step-by-step identity verification process and low-friction tools, like form auto-fill and passwordless authentication augment layers of passive security (fraud detection, data validation, etc) that run silently in the background to minimize the customer's burden of proof. With minimal friction and a welcoming UI, customers are able to quickly and easily complete enrollment.

Case study: account opening fraud

A leading US bank turned to Transmit Security when under attack by registration bots. The bank previously used 3 fraud detection tools that had overlooked 10,000+ fraudulent accounts in just one month. Transmit Security enabled the bank to retire two legacy vendors and achieve better outcomes:

1300%
ROI

500%
increase in bot detection

98%
reduction in AO fraud

90%
reduction in false positives/negatives

80%
lower operational costs

80%
reduction in friction & MFA challenges

A complete AO use case out of the box

A unified account opening platform provides everything you need to establish a secure, compliant and smooth onboarding process. Highly accurate, automated AO fraud protection simultaneously improves the customer experience — so you can cut fraud losses, onboard more customers and boost revenue.

- **Orchestration:** Omnichannel identity decisioning and workflows
- **Fraud Detection:** Fraud identity network, fraud ring, deepfake attacks, risk detection
- **Identity Proofing:** Document verification, face matching, liveness check
- **Data Validation:** Proof of address, email/phone verification, AML initial screening, goverment DBs
- **Authentication:** Passwordless, passkeys & MFAs
- **Identity Management:** Register user profiles

With a layered, plug-and-play AO solution, you gain full platform synergies to quickly adapt to risk, trust and evolving AO fraud tactics. Cloud-native capabilities work in concert to deliver the agility, simplicity, speed and accuracy you need — along with the cost-efficiency and limitless scale to enroll millions of customers.

Explore our platform