transmit security

USE CASE

End-to-End Fraud Management

The need for end-to-end fraud management capabilities

In the world of fraud management, detection is only the tip of the iceberg. Fraud analysts shoulder the critical responsibilities of proactive protection, case management, investigation, reporting and orchestrating responses that mitigate real-time threats. Too often, addressing these many tasks can lead to a high cost of ownership.

These costs are increased when analysts must manage numerous solutions, not only for real-time detection, but the full spectrum of fraud operations tasks, multiplying the time and expertise needed to train new members and resolve fraud cases — especially in scenarios that demand manual processes and analysis.

To reduce these costs and ensure a robust defense against fraudulent activities, anti-fraud teams require a consolidated, comprehensive solution for end-to-end fraud management. This paper illustrates how Transmit Security's anti-fraud solution helps teams overcome the challenges of fraud management, reduces ownership costs and empowers analysts to safeguard customers in a holistic manner.

Beyond real-time detection: The challenges of case management

Although real-time detection and response tools provide a crucial first line of defense against attempted fraud, certain fraud cases still demand manual review in addition to — or instead of — automated responses to detected anomalies.

This not only includes scenarios where manual analysis is mandated by regulatory requirements, but other scenarios, such as:

Customer-initiated cases: Customers who report suspected fraud or account blocking require manual case investigation to determine the validity of their complaints. These cases must be quickly resolved to avoid loss of trust or damage to brand reputation.

False positives and negatives: Real-time fraud detection solutions are only as good as the data they are trained on, often leading to false positives and negatives for new and complex threats. Human analysis can keep fraudsters from evading detection and prevent loss of business due to inaccurate detection that can degrade customer experience and block new customers from registering.

Gray areas and ambiguities: Some transactions or behaviors fall into gray zones that require investigation from human experts in order to make an informed judgment and provide feedback for real-time detection systems.

To address these scenarios and the full range of tasks needed for end-to-end fraud management, analysts rely on a bevy of solutions, including:

- **Case management systems** for logging, tracking and reporting the actions taken to resolve cases that require manual investigation.
- **Analytics and visualization solutions** to extract data from multiple systems or build visualizations that correlate risk signals from multiple proprietary solutions, databases and web services.
- **Offline analysis tools**, which analyze large datasets that would be too resource intensive for real-time processing, enabling better detection of connected cases, such as fraud rings and large-scale parallel attacks.
- **Productivity platforms** such as Slack, Jira and other software for communication, task delegation and collaboration within and across teams.
- **Orchestration services** to integrate and standardize signals from multiple systems and build journeys to automate responses based on a unified calculation of risk.

Time, expertise and operational resources are needed to integrate and maintain these various systems, and tedious manual work is often required to cross-correlate and standardize data from various sources. This can lead to gaps in detection that reduce the efficacy of fraud management and ongoing challenges that increase cost of ownership.

Each additional tool also increases the time needed to train new team members and the complexity of internal processes — such as assigning and prioritizing tasks, establishing procedures for escalating cases and creating playbooks for future attack scenarios.

End-to-end fraud management doesn't stop at real-time detection — it requires:

- ✓ Internal processes for ownership and actionability
- ✓ Unifying data and tracking progress for individual cases
- ✓ Analyzing data from multiple sources to understand fraud patterns
- ✓ Filtering real-time alerts to triage high-priority cases and large-scale attacks
- ✓ Building visualizations for fraud rings and attack MOs (modus operandi)
- ✓ Risk-and-trust orchestration to unify risk decisioning and optimize risk-based journeys
- ✓ Tuning decisioning, updating security mechanisms and preparing for future attacks

How a unified fraud management solution reduces costs and improves operations

Transmit Security provides a comprehensive solution that gives analysts everything they need for end-to-end fraud management in a single solution — streamlining fraud operations by simplifying, expediting and automating a wide range of tasks. This dramatically reduces the operational costs associated with licensing, maintaining and integrating numerous systems that require complex development efforts and time-consuming data correlation.

And as teams are able to consolidate solutions and reduce manual tasks, they can reduce time to mitigation and close gaps in detection that result from data silos.

Our holistic anti-fraud solution enables analysts to:

Make swift, high-impact actions through offline analysis: Reduce the time and manual data correlation needed to detect and mitigate connected cases using link analysis to visualize fraud rings and campaign detection that clusters alerts and unifies information related to parallel attacks. Offline analysis provides a cost-effective way to analyze large-scale datasets, expediting teams' ability to prioritize investigations, understand connected cases and adapt to shifting fraud patterns over time.

Simplify investigations with unified visibility and AI-based analytics: Gain fast access to the most relevant information for investigations with custom dashboards that let you view all risk signals in one place. Reduce analysts' reliance on developers to interpret, update and document mitigation efforts with generative AI-based analytics, which enable data analysis via natural language queries, returning text or visualizations that synthesize data from multiple IDPs, databases and detection services.

Expedite resolution with end-to-end case management capabilities: Save time by unifying all the data for each case into a single pane of glass that charts the risk signals along each step in the user journey within the UI, with tools that facilitate tracking and collaboration. Simplify reporting and actionability with explainability for the top factors that indicate suspicious behavior and the ability to automatically block known fraudulent entities to prevent future attacks.

Streamline internal processes with automated workflows: Eliminate the inefficiencies that result from inconsistent or undefined internal processes with fraud operations playbooks. Give experts the time to focus on complex investigation and analysis by integrating with third-party tools to automate repetitive tasks and workflows, and reduce time to resolution by creating workflows on demand that automate response strategies for future attacks.

Reduce development efforts with orchestration: Streamline and simplify the development of risk-based decisioning and journeys with low-code tools that unify and standardize risk signals from any natively integrated or third-party service. Shrink the time needed to analyze and optimize KPIs by testing and deploying multiple policy versions in parallel, and address the entire user lifecycle with orchestration built into a complete customer identity and access management platform.

Managing fraud across the user lifecycle

Fraudsters can strike at any time in the user journey, requiring the ability to pinpoint, challenge and block suspicious activity at each step along the way. This requires a multilayered identity security strategy that uses data validation, authorization, authentication and identity verification capabilities to strengthen digital onboarding, implement risk-based authentication, secure payments and improve account recovery.

However, risk signals across the user journey — such as failed OTPs, multiple authentication attempts or suspicious IDs — are often siloed within different solutions from different vendors. As a result, complex data correlation is needed to understand, document and resolve a single fraud case. This is even more challenging when solutions require thousands of lines of custom code to build risk-based journeys or rely on black-box detection mechanisms that provide no insight into their recommendations to block, challenge or allow each request.

Transmit Security solves this challenge by giving analysts an end-to-end view of each customer's entire journey, allowing them to trace the risk detected in each platform module for each fraud case, from the user's first interaction to their last, with clear explanations into the specific risk indicators detected by each component in the security stack.

Here's how it works:

01 Risk signals are collected using prebuilt connectors to external data sources or natively integrated services that leverage hundreds of detection mechanisms to pinpoint anomalies across the full user journey, based on the user's historical behavior.

02 For each suspicious request, analysts can access a single pane of glass view that provides full visibility into the end user details, ID photo (if applicable) and a step-by-step view of their user journey with risk signals from each service in the identity stack, such as age mismatch during identity verification or OTP failure during authentication.

03 Within the UI, analysts can access everything they need to investigate and document anomalous patterns, manually approve or reject requests, use tracking and messaging tools that pull data from external sources and enable updates through Slack, Jira or other internal tools — and more.

04 For confirmed fraud cases, analysts can mark emails, selfies, passkeys and IPs as fraudulent to automatically reject future requests that contain these components. These labels can also be fed into third-party systems to trigger downstream processes, expediting resolution of future cases.

05 Additional features — including a Labels API for self-service feedback loops and a detection sensitivity interface to customize the threshold for real-time detection of suspicious behavior — allow analysts to use their findings to instantly tune decisioning mechanisms without the need for complex development efforts.

Put analysts at the center of anti-fraud operations

Ultimately, anti-fraud solutions that focus only on real-time detection fail to understand the complex efforts needed for fraud operations. This results in a proliferation of siloed tools that escalate operational costs due to licensing expenses and the many man hours needed to integrate and manage them. And as sophisticated fraud MOs become commonplace, these costs will only increase due to the complex data correlation needed to resolve difficult cases.

By providing a comprehensive, analyst-centric solution, Transmit Security empowers teams of any size or skill level to enhance detection while reducing the cost of ownership. With the ability to automate tedious tasks, cut down on noisy alerts, instantly provide feedback and streamline documentation, small teams and novice analysts can minimize complexity, while large teams and experts can deliver world-class operations by fine-tuning decisioning and orchestration.

To find out more about how Transmit Security can transform end-to-end fraud management at your enterprise, contact Sales to set up a free demo.

Explore our platform