Outseer Fraud Manager™

Account protection from login to payment

OUTSEER

Stop Fraud Not Customers®

One Solution, Complete Protection: From Login to Transaction and Everywhere In-Between

Rapid changes in digital banking and online payments coupled with the rise in popularity of real-time payments (RTP) are exposing vulnerabilities that fraudsters are quick to exploit. Fraudsters are looking for the weakest link in your fraud prevention strategy, and fighting fraud in silos weakens your defense. Connecting the dots between risk signals at every step of the digital journey can help your organization achieve the perfect balance between securing your customer's accounts and providing them with the superior user experience they deserve.

The surge in RTP in particular has led to rising threats with fraudsters exploiting the speed of these payment rails for quick cash outs. While scams and authorized pushed payments (APP) are on the rise, account takeover remains a significant threat vector. In fact, recent **Datos Insights**[1] research shows that 71% of fraud executives indicated an increase in account takeover attacks over RTP rails. Connecting the dots from login to a transaction and holistically assessing the risk of each step of your customer's digital journey is more important than ever.

Superior Data Science for Superior Results

- Leverage insights proven in the highest threat environments

- Defend against the latest fraud trends with our unique consortium data

- Benefit from risk models trained on trillions of transactions at the world's largest financial institutions

Leverage a common Fraud Management Platform throughout the customer journey

- Connect insights across authentication and payment transactions

- Enrich risk scoring by ingesting first-party and third-party data signals

- Deliver consistent risk mitigation controls and experiences at every customer touchpoint

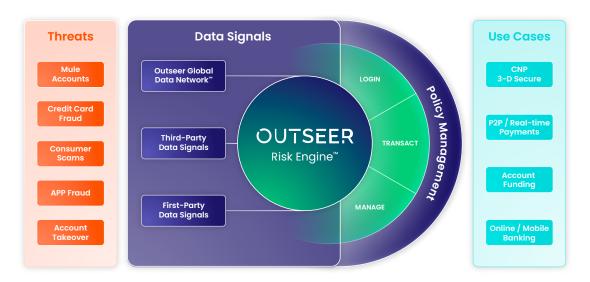## Optimize customer experience and operational efficiencies

- Use normalized risk scores to balance your fraud, customer experience, and operational costs

- Implement policy changes in response to evolving threats

- Collaborate with our experts for continuous improvements and peer benchmarking

---

[1] Datos Insights (formerly Aite-Novarica). "Faster Payments, Faster Fraud: Solutions to Stop the Madness." **https://www.outseer.com/aite-faster-payments/**, May 2023.

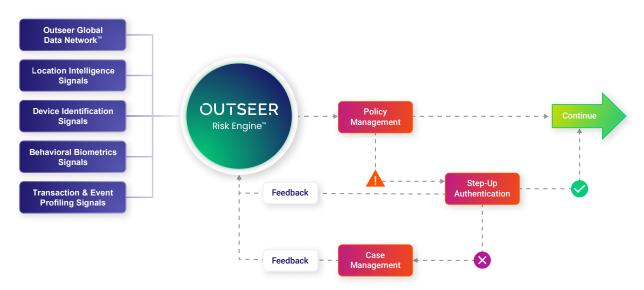# Helping You Protect Every Step of the Customer Digital Journey

The Outseer Platform, which underlines Outseer Fraud Manager, is a proven transactional risk management platform that enables our customers to protect digital transactions from login to payment completion. Outseer customers benefit from streamlined operations, reduced account takeover risk, and lower fraud losses while maintaining an exceptional consumer experience.

The Outseer Platform is powered by the Outseer Risk Engine™. Built for precision detection, it utilizes the most effective models and data to detect and prevent fraudulent activity. Our predictive algorithms work in real-time, and at a high-volume scale, analyzing transaction data, our unique consortium data signals from the Outseer Global Data Network™, and first- and third-party signals. Our risk models are trained on billions of transactions at the world's largest financial institutions.

How It Works

Outseer Fraud Manager is powered by the Outseer Risk Engine that accurately assesses the risk associated with each transaction and digital interaction during the user's digital journey. By applying a risk-based approach, only a small number of activities or transactions require additional authentication that can be done using consistent, out-of-the-box step-up authentication options or by leveraging the organization's authentication tools.

Outseer Risk Engine

The Outseer Risk Engine is at the core of the Outseer Platform and is built for precision detection. Our proven risk models have been trained on trillions of transactions to deliver the highest risk score accuracy. The Outseer Risk Engine analyzes hundreds of signals coming from transaction data, the Outseer Global Data Network, third-party signals, and first-party signals and uses predictive algorithms to detect and prevent fraud in real time. Using an advanced machine learning statistical approach to calculate the risk score, it looks at the conditional probability of each event to evaluate if it's most likely genuine or fraudulent given the known facts or predictors. All available signals are taken into consideration but weighted according to correlation with fraud—the most predictive signals contribute more heavily to the score. The predictive weighting calculations are updated for each unique customer based on authentication results and case management feedback. Unlike black-box risk engines, Outseer delivers reason codes for top contributors of a score for explainable results. Our normalized risk score gives you the predictability you need to confidently choose the risk score thresholds that meet your business objectives and risk appetite.

Outseer Global Data Network

Outseer Fraud Manager uniquely benefits from data signals contributed by the Outseer Global Data Network—a globally shared, fraud intelligence consortium that gathers data from transactions spanning thousands of financial institutions worldwide. When a member of the network marks an activity as "Confirmed Fraud" / "Confirmed Genuine" in the case management application the associated signals are shared across the network. When an activity is attempted and includes one of the signals from the Outseer Global Data Network the risk is automatically adjusted, in addition, our customers can define rules that leverage facts such as "Is this signal in the Global Data Network?"

Device Profiling

Outseer's device profiling capabilities allow you to assess whether a customer's device is different than one usually used to conduct business with your organization or if it has been connected to known fraudulent activities. This assessment involves analyzing parameters such as IP address, geolocation, operating system, browser type, and other device settings. In many cases, account takeover attacks are conducted from fraudsters' devices using genuine user credentials. Therefore, accurate device identification and profiling of known devices for a user is key to mitigating account takeover. Outseer device profiling and device identification capabilities use an unsupervised machine learning algorithm to calculate an accurate assurance level that reflects the probability the user used the device in the past.

Behavioral Analytics Profiling

Our behavioral profiling compares current session activity with established customer behavior to detect deviations that may be indicative of fraud. Multiple signals are examined including frequency, time of day, and type of activity. (e.g., Are these payment types and associated transaction attributes consistent with typical transactions for this user?)

Protection For Mobile Users

Outseer Fraud Manager enables a secure and frictionless mobile experience by leveraging Outseer Fraud Manager Mobile SDK available for both iOS and Android devices. This SDK integrates with your mobile application, collects mobile device identifiers for risk assessment, and invokes biometrics and OTP push notifications as step-up authentication for flagged transactions.

Outseer Case Management

Our case management application enables you to monitor activities that trigger policy and confirm if they are fraudulent. It also allows you to tag activities based on the attack vector for further analysis (e.g., scam/not scam). The web-based application enables you to research activities and analyze fraud patterns, for instance when revising or developing new policies. When cases are confirmed to be fraudulent, feedback is instantly provided to the Outseer Risk Engine to further enhance the risk analysis accuracy. An API is available that allows the consumption of third-party case data and exporting of cases and activities to third-party case management applications.

Outseer Policy Management

The Outseer policy engine translates data signals and risk intelligence into action. Using our fine-grained policy controls, you can set different outcomes to different risk thresholds based on your risk tolerance and your business objectives. The web-based Outseer Fraud Manager Policy Management application allows you to set event-level policies, such as policies that will only trigger at payment, at login, or when a user is managing their account settings. No coding is required to define a policy. You simply click and select the elements you want to include as part of the policy logic.

Orchestration Capabilities

Outseer's platform can help your organization orchestrate your fraud prevention and authentication efforts by centralizing your fraud management, maximizing your investment in different fraud prevention tools, and enhancing your fraud detection. Our platform provides the flexibility to build granular policies for different events in the customer journey that result in different actions and leverage first- or third-party signals. Outseer platform provides an interface for integrating with other vendors, such integrations include:

- Third-party signals that impact the Outseer Risk Engine risk score calculation

- Third-party signals flowing through to the policy management application

- Third-party step-up authentication options

Step-Up Authentication

An additional layer of step-up authentication may be employed to further validate one's identity in high-risk scenarios or scenarios that violate your organization's policies.

Challenge questions: questions selected and answered by the user during enrollment

Out-of-band authentication: one-time passcode sent to the user via text message, phone call, or push notification

Biometrics: fingerprint and face ID biometrics based on the mobile operating system technology (available for mobile application users)

Transaction signing: Crcryptographically signs transaction details to verify transaction integrity and authenticity to fight advanced financial malware attacks

Authentication orchestration framework for external authentication allows bring-your-own-authentication methods, such as tokens or FIDO-compliant biometrics and passwordless authentication methods

Streamline Your Fraud Prevention Efforts with a Proven Fraud Management Platform

Outseer Fraud Manager leverages its heritage as a pioneer in science-driven innovation to support risk management and fraud prevention solutions. Outseer's superior data science can help your organization reduce fraud losses while optimizing customer experience and operational efficiencies.

Outseer Fraud Manager allows you to streamline insights across authentication and payment transactions while delivering consistent risk controls at all customer touchpoints. It helps you leverage your investment in other fraud tools and provides you with an enhanced risk score ingesting first- and third-party data signals into one score. Our normalized risk scores allow you to predict your fraud, customer experience, and operational costs balance. Enabling you to quickly deploy policy changes in response to rapidly evolving fraud trends and regulatory requirements.

About Outseer

At Outseer, we are empowering our customers to liberate the world from digital fraud by providing solutions that stop fraud, not customers. Our market-leading fraud and authentication platform is used by thousands of financial institutions around the world to protect millions of customer accounts and billions of transactions annually. Leveraging proven data science, including our proprietary consortium data, our customers use our risk-based, machine learning platform to deliver the highest fraud detection rates, lowest false positive rates, and lowest customer intervention in the industry. See what others can't at **outseer.com**.