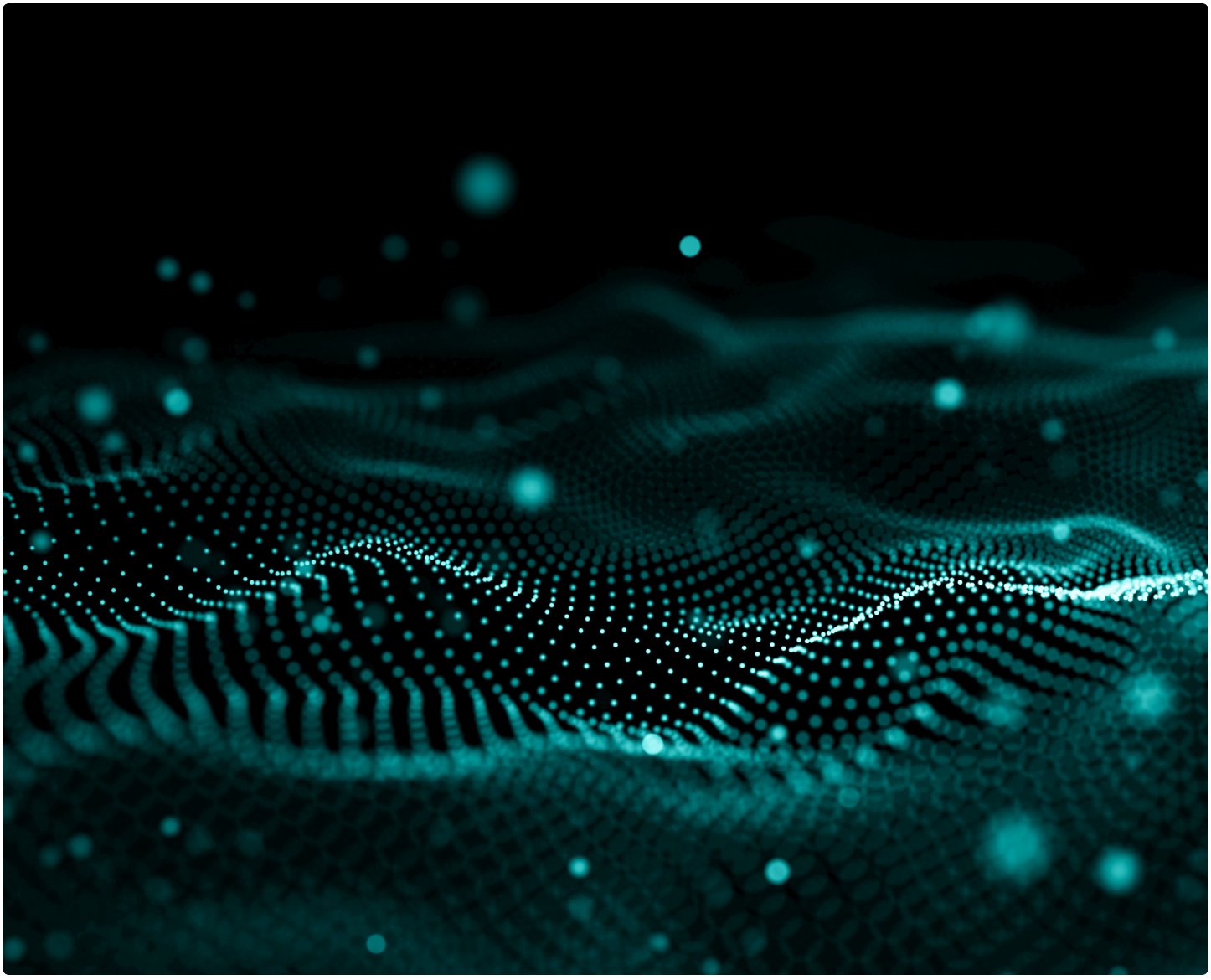
Palantir

Palantir Foundry for Transaction Monitoring

Palantir Technologies
→ palantir.com



Palantir

Introduction

The landscape of financial crime has evolved significantly in recent years. The brute force criminal tactics of the past have given way to far more sophisticated criminal activity; modern financial criminals are data-driven and focused primarily on exploiting the gaps created by ineffective, inefficient systems. Both social engineering and data engineering play a major role in financial crime, and threats are constantly growing in scope and complexity. Using new payment technologies, like cryptocurrencies, mobile payments, and near real-time payment services, criminals have more avenues to commit crime and take advantage of system vulnerabilities than they had before.

At the same time, financial institutions have struggled to keep up with the growing threat landscape. They largely resort to using point technologies and single-issue countermeasures instead of flexible and holistic tools that leverage machine learning and artificial intelligence. Institutions can't adequately monitor for, and flag, an ever-increasing number of suspicious transactions using these legacy tactics.

The need for a holistic and AI-driven transaction monitoring solution only becomes more apparent when taking a look at the challenges that many financial institutions face when it comes to traditional anomaly detection strategies.

These challenges include:

01 **Moving beyond static rule sets** →

How do I more accurately flag suspicious transactions?

Financial institutions have long relied on static rule sets to cover traditional methods of anomaly detection. This has led to rule creep, bias, and stale rule sets that over-alert and underperform.

02 **Manual and siloed workflows** →

How do I streamline workflows and enable collaboration across teams and systems?

To monitor transactions effectively, organizations must collate data from many sources — data that's often in different formats or comes in at different cadences — and make decisions based on multiple teams' analyses. Additionally, financial institutions may tend to use a fixed, rather than a dynamic, data model, in which data about what crimes are occurring, when they're happening, and who's committing them is fed in batches rather than in real time. This means that at any given time, companies may be missing out on a holistic, up-to-the-minute view of criminal activity, which doesn't help them proactively impose sanctions or limits to stop crimes from occurring.

03 **Operationalizing scenarios and risk modeling** →

How do I take the models I've developed and efficiently put them into production?

Every day, financial risk analysts put together and refine models designed to sift through data and better identify suspicious behavior. These models are not useful on their own, though: what's required is an interplay between the data, the models, and decisions made. Because organizations often lack a trustworthy data foundation, full-fidelity feedback loops between consumers and model builders, safe mechanisms for writing back to systems of action, and shared security and lineage frameworks across teams, they may find it challenging to actually make the most of their data models.

04 Keeping track of policies and controls →

How do I properly audit and report on suspicious transactions to ensure that I am meeting my regulatory requirements?

Beyond identification, a key aspect of transaction monitoring is reporting suspicious transactions to regulatory bodies and tracking what works and what doesn't work over time. This requires narrative generation, automatic feedback loops based on granular analyst feedback, and the creation of an auditable trail of all cases and filings.

Proven technology to improve highly complex transaction monitoring processes

Foundry has been deployed across many of the world's largest financial institutions. Our customers have managed to lower their costs by 90%, improve their true positive rate by 40x, and cut their investigative time in half — all while improving their risk posture and regulatory relationships.

From banking giants to fast-rising fintechs to regulators, companies globally trust Palantir Foundry to automate and accelerate their anti-financial crime efforts, especially in the area of transaction monitoring.

At its core, Foundry is a decision orchestration platform. It enables organizations to integrate all of their data from different systems, use that data to fuel decisions, and derive insights from the decisions made and actions taken to improve operations over time. Foundry was built for highly complex environments like financial institutions, enabling data scientists and analysts to work hand-in-hand on highly involved workflows. The platform enables compliance organizations to move from a rigid, overly structured, rules-based approach to transaction monitoring to more flexible and information-inclusive processes.

From building a unified customer profile to enabling AI-assisted triage and evidence generation to managing all aspects of cases, including regulatory reporting, Foundry provides a comprehensive solution to every aspect of transaction monitoring. Using the platform, analysts can make more informed decisions, faster, with greater insight into customers and their networks and the automation of numerous workflows.

Foundry is designed not for a single, specific use case, but rather for a virtually infinite range of data sources, use cases, and users. As a result, financial institutions can build or bring a suite of dynamic risk models, complex automation models, and versatile applications into Foundry. This approach to building a comprehensive platform, instead of a series of siloed solutions, reduces the total cost of ownership, since each incremental use case or workflow is significantly less to implement than if an organization used a disparate set of systems.

Because Foundry acts as a central hub for all of your data, including transaction details, lists of sanctions, information from corporate registries, and even negative news, all of the information critical to your transaction monitoring efforts is stored in one central place. Financial institutions own the work and IP (intellectual property) within the platform, as well as any applications developed within Foundry. With full control and ownership over their data and workflows, banks and regulators can confidently keep up

with the sophistication of criminals and regulatory requirements. Of course, Foundry for AML incorporates privacy and security into every operational capability, with purpose-based access controls, the propagation of security "markings" on every asset, and strict adherence to data protection laws.

Why Palantir Foundry for Transaction Monitoring?

Build a holistic customer profile

The more you know about your customers, the easier it is to spot suspicious behavior. Unfortunately, financial institutions using legacy technology frequently find it challenging to get a unified view of every customer. Customer information is often stored across different systems in difficult-to-parse formats, so seeing the whole picture means that analysts need to review information across siloed data sources. Cleaning and migrating this data into various point systems for analysis requires a large amount of work, which tends to increase the likelihood of lock-in (thereby perpetuating the problem). Additionally, legacy systems only support fixed, rather than dynamic, data elements, and aren't designed with transaction monitoring in mind, so implementing controls based on the information proves challenging.

All in all, not having a single birds' eye view of all customer activity makes transaction monitoring a manual, error-prone, and imperfect practice.

Foundry was designed to help organizations of all kinds, including financial institutions, bring all of their data sources together. Foundry has over 200 out-of-the-box connectors to get data from fragmented systems — like your core banking systems, existing anomaly detection systems, third party watchlists, corporate systems and devices, and more — into a single place for ongoing analysis. APIs and RPA (robotic process automation) help you build a more complete unified customer profile. AI-driven data pipeline generation and normalization, data cleaning, and full visibility into the lineage of your data all make data integration more seamless.

Effective transaction monitoring also requires you to get a complete sense of all the other entities connected to your customers, as determined by matching physical addresses, IP addresses, device IDs, phone numbers, and common transactions. Foundry's entity resolution engine and network building models enable you to get a 360° view of your customers' networks, including all relevant accounts and transactions related to that customer. For instance, you might want to track not only the financial flows between one of your customers and their business partner, but also the device located in a high-risk jurisdiction that the business partner frequently sends money to.

Palantir

Based on these details, Foundry generates an overall behavioral risk score, providing a single metric incorporating transaction behavior, KYC information, and third party data. These capabilities can help you identify circular flows of funds, suspicious UBOs and shell companies, SAR networks, and risks by association.

Foundry's Ontology acts as an operating layer within the organization, making the integration and consolidation of data and models possible. The Ontology captures not just all of the aforementioned data but also the decisions and actions taken by analysts and other decision-makers. In this way, the Ontology serves as a true digital twin for an institution and makes anomaly detection into a truly holistic process.

No two financial institutions are the same, so Foundry offers flexibility when it comes to risk management based on your needs. The platform allows you to modulate the signal-to-noise ratio of incoming feeds in alignment with your anti-financial crime risk policies; you can modify the sensitivity of Foundry's transaction monitoring based on your requirements. Additionally, the Ontology enables non-technical analysts to quickly configure the platform without having to write custom code.

Foundry makes it seamless for financial institutions to combine all necessary data sources and understand your customers, as well as their networks. This can provide the right foundation for understanding risk and making critical decisions.

Enable AI-assisted triage and evidence generation

As the number of products, customers, geographies, and accounts managed by a financial institution grows, so does the need for greater efficiency in transaction monitoring. Indeed, one of the biggest challenges that operational anti-financial crime analysts face with traditional transaction monitoring solutions is limited automation capabilities. Analysts need to deal with an ever-growing volume of alerts, risking "investigator fatigue," and most of the alerts don't actually constitute fraud.

It's not just the sheer number of alerts, though: legacy solutions often don't provide enough detail in the alerts themselves for analysts to know whether to confirm or deny anomalous behavior. Blacklisting and whitelisting alerts based on static rules simply doesn't work due to the rules' simplistic nature, creating more headaches.

Because data isn't centralized, analysts must manually hop between different internal and external systems, which not only wastes time but also introduces greater risk of errors. When it comes to generating evidence, this too often requires manual work: analysts need to write narratives and attach supporting documents.

A distinct lack of automation, coupled with incomplete alert information, plagues analysts and ultimately reduces the effectiveness of institutions' transaction monitoring efforts. Firms would benefit from a solution that can streamline much of the triage and evidence generation process and use what's learned through this workflow to improve operations over time.

The Foundry platform includes machine learning facilities that can intelligently augment the holistic customer profiles and risk profiles Foundry creates, while also automatically building an evidence trail. These narrative generation capabilities allow analysts to quickly see evidence that's been collated from previously siloed systems and make a quick decision. Foundry's machine learning capabilities also alert analysts to newly emerging evidence that may be related to an ongoing case investigation. Based on analysts' actions, this agent can also make recommendations on which kinds of alerts they may wish to suppress and how their risk posture may change in response. All of these features can reduce the burden on anti-financial crime analysts, helping increase their efficiency.

For alerts that do require a set of regulatory reports, Foundry can automatically send many of them straight through for verification, incorporating the body of evidence generated. Additionally, for confirmed matches, link/network analysis and risk ranking enable institutions to assess the financial risk that these fraudulent transactions pose.

Foundry's transaction monitoring capabilities only get more effective over time thanks to automatic feedback loops. As analysts verify the evidence that Foundry collects for specific customers, these verifications are fed back into the risk model, so future alerts that are similar in nature can be evidenced automatically and closed.

While Foundry makes it easy for data analysts to build models for detecting anomalies using FoundryML, it's equally as easy to import external models you may have built, or are currently building, in another tool, such as SageMaker, Azure ML, Google Cloud AutoML, or DataRobot. This flexibility makes Foundry exceptionally useful for financial institutions that have complex models already created.

To help institutions appropriately manage the sensitivity of their alert thresholds, Foundry supports automatic parallel runs using a champion challenger or A/B testing model. If, for instance, you wanted to change a scenario threshold, you could integrate alerts from your legacy transaction monitoring system and then let Foundry run using both the original threshold and the new one for a few months. At the end of this period, assuming there's sufficient evidence that none or only a small number of the old alerts warranted a SAR, you would be able to migrate to the new threshold with confidence.

Foundry offers significant efficiency improvements for some of the crucial workflows analysts use when monitoring for fraudulent transactions. These improvements can not only help save time, but also reduce the chances of user and technical errors.

360° alert and case management, through to regulatory reporting and operational actions

Once a transaction monitoring system flags anomalous activity, it is time for an analyst to jump in and determine whether the transaction was, indeed, fraudulent and report their findings appropriately. Following the right workflows is crucial, but many transaction monitoring solutions don't offer particularly helpful guidance. Even more importantly, these solutions oftentimes don't create a connecting loop between the analyst's final decisions and actions and the underlying AML or fraud identification mechanism. As a result, the system doesn't have the ability to learn dynamically over time and may make the same errors over and over again.

Foundry for AML helps simplify all aspects of alert and case management for analysts involved in transaction monitoring. Since analysts gain overall visibility into customer networks — not just the customers themselves, but also all of the entities they're connected to — they can see an overall risk score and use this information to detect more anomalies. Additionally, Foundry offers flexible and guided workflows to streamline processes for analysts and reduce the chance for error. For example, if the system notes that a potential instance of fraud is probably a false positive, it might route the case in a certain way, and based on the analyst's determination feed logic back into the data models appropriately. Analysts don't have to do a lot of this information routing themselves, which not only saves time but also helps protect against alert biases or poor training.

One of Foundry's key differentiators as a decision orchestration platform is its ability to create a closed loop between operators, decision-makers, and data analysts. This is made possible by the Foundry Ontology. In the anti-financial crime world, decision orchestration relies on the creation of feedback loops between the data scientists working on the data models and the analysts actually making day-to-day decisions about particular transactions. Organizations can also link different parts of the process together. For instance, Foundry can incorporate feedback from data analysts into core banking systems to block specific transaction or close accounts if those actions are warranted.

Institutions can use a suite of native data connectors, to enable bi-directional sync to third party and in-house tools, which can help firms gain a holistic, visual view of transactions and their connected entities. These tools can include standalone case management systems, network/link visualization tools, graph databases and third party systems for models. Once a decision is made, Foundry feeds the decisions back to the people designing the models, helping automate the acquisition of new data points and eliminating information siloes.

When it comes to regulatory reporting, Foundry helps automate these processes as well. You get automatic generation and filing of SARs and CTRs with relevant regulatory bodies, aided by the aforementioned narrative generation capabilities. Of course, Foundry always keeps an auditable trail of all cases and filings, so at any time you can go back and track how a case was managed through the process.

Palantir

Conclusion

Foundry for anti-financial crime helps analysts, data engineers, and regulators:

Anti-financial crime efforts, particularly those focused on transaction monitoring, are frequently error-prone, overly simplistic, siloed, and painfully manual. In designing Foundry, Palantir considered the biggest pain points that institutions face with anomaly detection and developed a solution that helps everyone involved in transaction monitoring become more efficient and effective.

01 **Spend their time identifying true risks instead of chasing down legitimate transactions** →

Foundry automates much of the work involved in detecting and flagging potentially fraudulent transactions. With comprehensive out-of-the-box modules, workflows, and models, as well as the flexibility to work with existing models and bring in data from other systems, Foundry lets you and your team focus on actual threats.

PROOF POINTS: →
- → Improve true positive rate by 40x
- → Using Foundry, an international bank saw 60% faster case resolution

02 **Reduce reliance on black box systems — and increase speed-to-deployment** →

Unlike many transaction monitoring solutions, Foundry is modular and open. A swath of connectors simplify bidirectional sync with third party data sources, enabling more complete customer profiles and advanced data integration. Additionally, Foundry plays well with external modeling tools. Foundry is easy to get started with — you can be up-and-running in one month — but also easy to customize, so institutions have a powerful base to build upon.

PROOF POINTS: →
- → On average, 1 month to deploy and customize
- → 70+ use cases

03 **Improve data quality and standardization** →

The average financial institution has a host of fragmented data sources to deal with, many from multiple entities. Foundry allows you to standardize processes across these disparate entities while also improving the data in upstream systems. Its best-in-class data integration, data quality, and security capabilities let organizations centrally store data from multiple entities while still retaining the ability to customize the data for each entity.

PROOF POINTS—AT AN INTERNATIONAL BANK: →
- → With Foundry, 4x as much data reuse
- → 4 billion data records were integrated resulting in ~90% faster and more consistent client information across jurisdictions

04

Enable collaboration between different teams →

Organizations that want to remain nimble must close the loop between anti-financial crime analysts, front-line customer representatives, and data scientists. Foundry makes it possible to keep all parts of the organization in sync and automate reporting to regulators.

PROOF POINTS—AT A LARGE EUROPEAN BANK: →

10x investigation productivity

→ 80% faster investigations, with ~20% more information reviewed at ~90% lower cost

LEARN MORE

↘

PALANTIR.COM/OFFERINGS/ANTI-MONEY-LAUNDERING/

Palantir Foundry unlocks a new approach to transaction monitoring with the flexibility to augment existing systems or orchestrate end-to-end workflows. Beyond transaction monitoring, Palantir powers anti-financial crime 360, KYC, and investigation workflows. This suite of solutions ensures financial institutions, fintechs, financial investigation units, and regulators alike can effectively and efficiently fight financial crime.