QUANTIFIND

WHITE PAPER

Monitoring Transactions is a Dead End

Why Payment Systems Demand a Paradigm Shift to Payments Risk Intelligence

This white paper will cover the following key areas:

Executive Summary: Brief overview, key takeaways, Call to action 1

The Source of the Problem 2

Introduction: The Ineffectiveness of Traditional Payments Risk Management 3

The Transaction Monitoring Conundrum 3

The Real Risk Alignment Approach 4

Today's Transaction Monitoring Process 5

The Limitations with the Greatest Impact 6

The need for a paradigm shift to Payments Risk Intelligence 6

The Benefits of Precise Language Models 7

The Quantifind Payments Risk Intelligence Approach 8

How to Assess Your Technology Choices 10

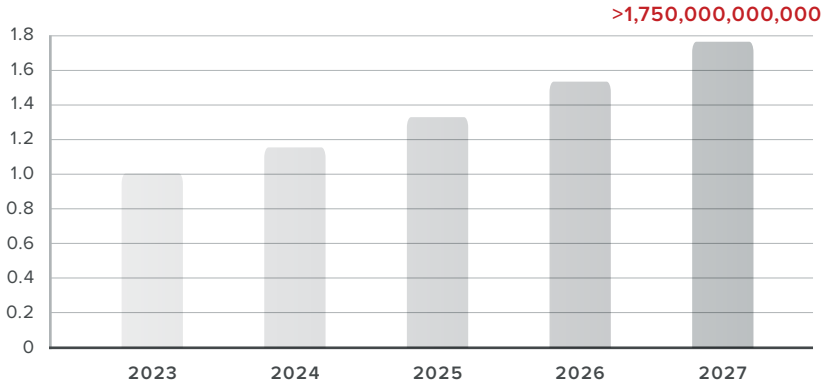
Public and Private Partnerships 11

Conclusion 11

Executive Summary

Monitoring transactions cannot scale to tomorrow's volumes. According to the Capgemini World Payments Report, non-cash transaction volumes surpassed 1 trillion globally in 2023, with projections indicating an annual growth rate of approximately 15% through 2027.* This surge in transaction volume and complexity presents significant challenges for traditional payment risk management approaches, which have long been the backbone of Anti-Money Laundering (AML) departments. These legacy systems, designed for a less dynamic environment, are increasingly inadequate in addressing the demands of today's fast-paced financial landscape. Risk programs often find themselves in a perpetual cycle of attempting to create order out of chaos, burdened by false alerts that impede analysts' ability to focus on genuine, complex threats. **This white paper is essential reading for AML and KYC risk management professionals seeking to scale their risk programs to meet the increasing volumes of digital payments and effectively combat financial crimes in a rapidly evolving landscape.**

***Projected Growth of Non-Cash Transaction Volumes**
(in Trillions)



The Source of the Problem

Looking closely at traditional payment risk management, one often finds two extreme ends of the spectrum. Sanctions enforcement is on one end, focusing on screening transactions for compliance with international sanctions. Traditional transaction screening methods are often ineffective due to their high rate of false positives. The static nature of screening rules means they can be easily circumvented by sophisticated criminals who adjust their tactics to avoid detection. The reliance on predefined lists also limits the system's ability to adapt to new and emerging threats.

On the other end of the spectrum are transaction monitoring solutions. These applications have significant limitations that undermine their effectiveness in detecting and preventing financial crimes. Typically implemented as on-premises solutions, they rely on static rules and simplistic AML scenarios that also result in a high volume of false positives. Traditional monitoring is reactive and periodic, failing to adapt to evolving money laundering techniques and allowing criminals to exploit gaps between monitoring periods.

Transaction Screening for Sanctions

Real-time

Limited view of risk focused on sanctions enforcement

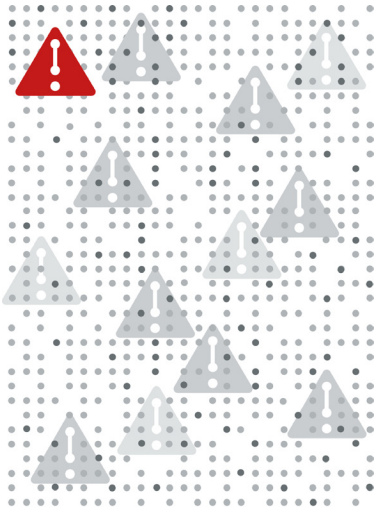
Each transaction assessed independently of all others

Demanding SLAs relegate "investigations" to name comparisons

Can be 10,000 or more false positives for every true positive

The Gap: True AML Risks

Hidden threats are not detected



Transaction Monitoring for Traditional AML Scenarios

Lagging behind payment execution, often with growing backlogs

ML detection scenarios originally designed for different payments environment

Antiquated scenarios trigger on modern customer behavior

Ignore counterparties and counterparty risk

No external context; based entirely on transaction behavior

Continue to miss true ML risks in payments

[1] *Capgemini World Payments Report 2023. (2023). Capgemini Research Institute. Retrieved from https://www.capgemini.com/insights/research-library/world-payments-report/*

The approach to Payments Risk Management has largely remained unchanged, but with the surge in digital payments, AML teams must evolve their methods to improve their effectiveness significantly. This paper introduces an advanced strategy that leverages purpose-built artificial intelligence to analyze customer relationships and identify hidden risks with Quantifind Payments Risk Intelligence. This approach shifts from looking at unusual activity from legitimate customers to focusing on counterparties and customers of concern by leveraging open-source signals. This new method offers greater accuracy and scalability, ensuring financial institutions can effectively combat financial crime risks.

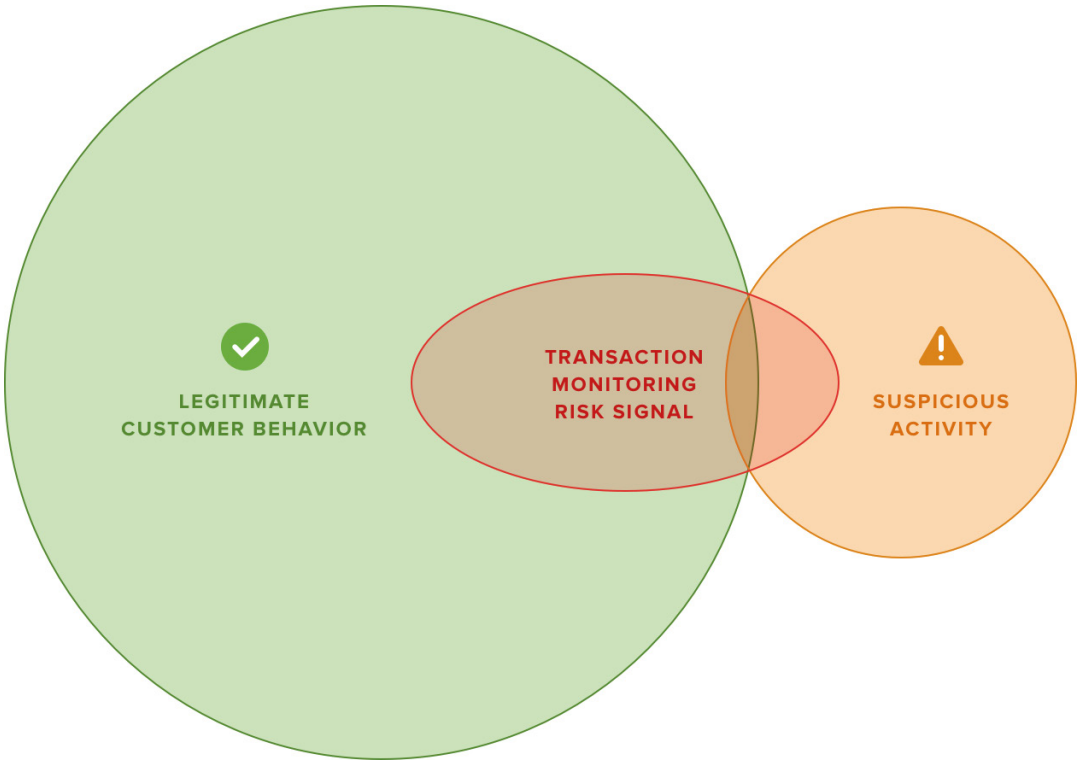
Introduction: The Ineffectiveness of Traditional Payments Risk Management

Traditional payment risk management systems rely on rigid rules and simplistic, historical money laundering scenarios that miss true financial crime. These antiquated scenarios often overlap with modern, legitimate customer behavior, causing many false positives and missed genuine threats. Consequently, resources are drained, operational inefficiencies arise, and sophisticated financial crime schemes go undetected. Additionally, the lack of contextual analysis in counterparty relationships means transactions are assessed in isolation, missing patterns and connections that could indicate risk.

Moreover, traditional transaction monitoring systems struggle to scale effectively with increasing transaction volumes. Traditional transaction monitoring applications face significant technical limitations that impede their scalability and effectiveness in the modern financial environment. These systems are typically built for on-premise deployment, relying on fixed hardware resources that cannot scale to accommodate the unprecedented increases in transaction volumes. As transaction volumes grow, these systems struggle to keep up, leading to performance bottlenecks and delays. Additionally, these applications are often designed to operate over traditional relational databases which are not optimized for handling the vast and complex data sets associated with contemporary financial transactions. As the system is stretched to its limits, it requires an increasingly larger share of the IT budget to maintain, diverting resources away from other critical areas. This inflexibility and high maintenance cost make traditional transaction monitoring applications ill-suited for today's dynamic and high-volume payment processing demands.

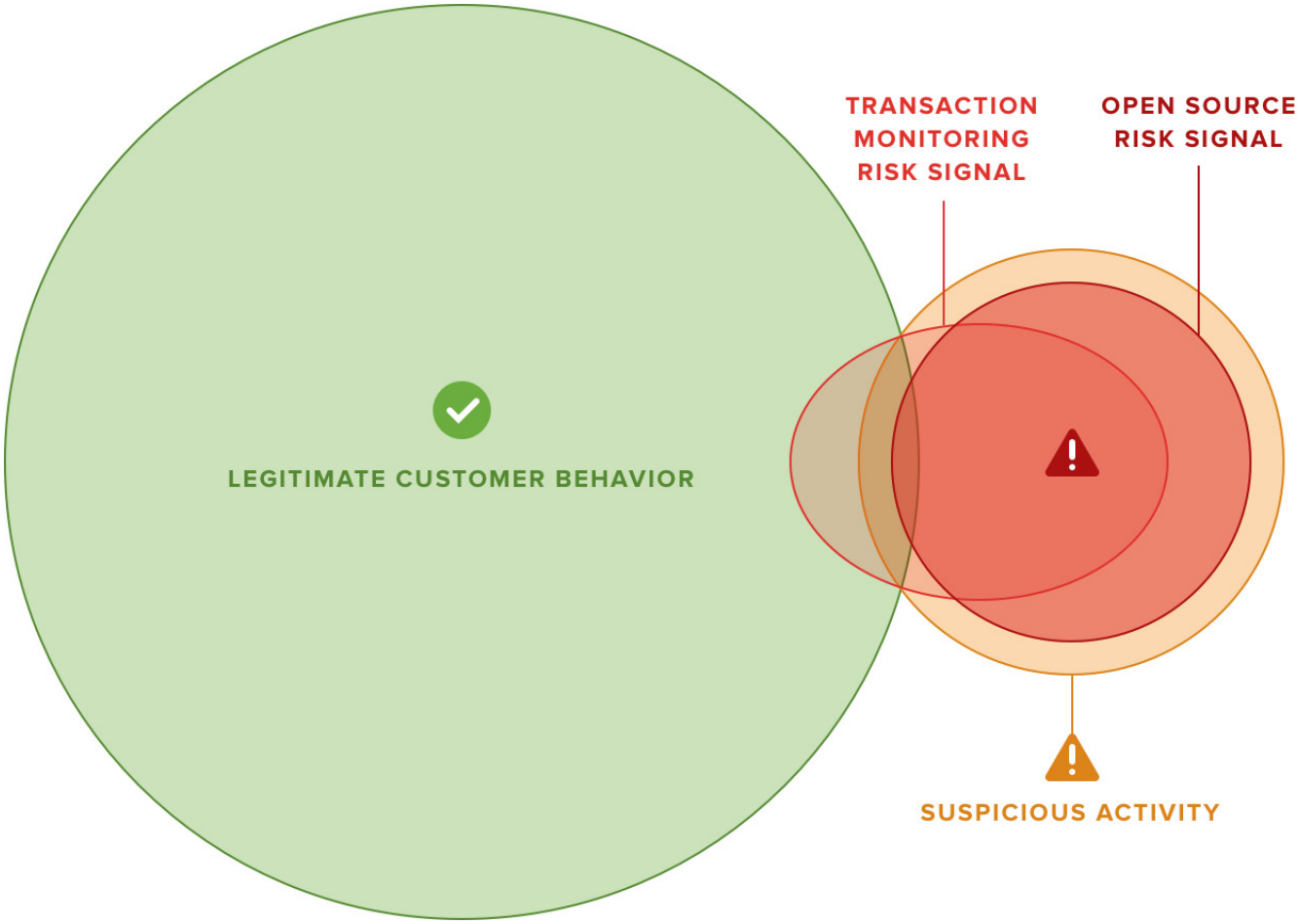
The Transaction Monitoring Conundrum

A legacy transaction monitoring approach misses hidden patterns and instead triggers illegitimate risk on legitimate customer behavior, causing many false positives and inefficiency.



The Real Risk Signal Alignment Approach

The real risk signal approach leverages Quantifind's risk intelligence to discover risk in relationships and monitor and investigate who you're doing business with.



Today's Transaction Monitoring Process is Backward

The problem with the legacy transaction monitoring process lies in its reactive and fragmented approach. This traditional method starts by examining transaction activity, monitoring for anomalies based on static rules, and then having analysts investigate the alerts generated. While this approach can catch some suspicious activities, it leads to significant inefficiencies, including high volumes of false positives that waste resources and false negatives that allow undetected financial crime. By assessing transactions in isolation, traditional systems lack the contextual understanding to identify complex patterns. Consequently, this method results in a reactive posture, addressing risks only after they occur. It fails to provide a comprehensive view of customer behavior and relationships crucial for accurate risk assessment and effective prevention.

Traditional Process

Transaction Aggregation

- Cash Profile
- Wire Profile
- ACH Profile

Transaction Monitoring

- Unusual cash activity
- Unusual wire activity
- Unusual ACH

Open Source Intelligence Investigation by the User

- Reactive triage of high alert volume
- Focus on risky counterparties or proving legitimate activity

A New Approach

Transaction Customer and Counterparty OSINT risk evaluation

- Identification of Open Risk typology signal confirmed by journalism, sanctions, court and arrest data, linkage to regulatory event
- Alignment to PEPs or Shell companies, nested business relationships linking to country risk
- LLM and Entity Resolution leveraging internal bank data and prior decisions.

Targeted Transaction profiling

- Review transactions linked to high risk parties MINIMIZE FOCUS on statistical outlier or risk patterns

Classic Reg Required Transaction Monitoring

- Cash Structuring
- High Risk Country Wires
- Round Dollars

Open Source Intelligence Investigation by the user

- Rapid collation of Risk Based OSINT already aligned to the alert
- OSINT collated for case and Suspicious Activity reporting

Limitations with the greatest impact to a payments risk management program:

Inability to Find Hidden Risks: Traditional transaction monitoring relies heavily on predefined rules, often too rigid to detect subtle and sophisticated financial crime patterns. These static rules focus on surface-level anomalies, missing the deeper, more complex interactions that could signal financial crimes. As a result, many financial crimes remain hidden, only to be discovered after significant damage.

Manual Review Burden: Traditional systems generate many alerts and many false positives. Each alert requires manual review by human analysts, which is time-consuming and labor-intensive. This manual approach strains resources and slows financial crime detection, allowing some financial crime transactions to go unnoticed until it is too late. The heavy reliance on manual intervention reduces the overall efficiency and responsiveness of the system.

Scalability Limitations: As transaction volumes grow, traditional systems face significant challenges in scaling. The technology and the manual review process cannot keep pace with the increasing number of transactions, leading to backlogs and delays. Traditional transaction monitoring systems rely on limited on-premises deployments versus more flexible cloud-based service models and traditional relational databases, making them incapable of scaling with increasing transaction volumes and leading to performance bottlenecks and delays. This inflexibility results in higher maintenance costs, diverting resources from other critical areas. Additionally, the speed at which these systems operate is insufficient for real-time financial crime detection, leaving financial institutions vulnerable to fast-moving financial crime schemes. The lack of scalability and speed hampers the ability to provide timely and effective risk management.

Fragmented Risk View: Data used in traditional systems is often siloed, limiting the ability to view risks across different channels and systems comprehensively. This fragmented approach hampers the ability to identify complex, multi-layered threats that span various data sources.

Reactive Rather Than Proactive: Traditional methods are predominantly reactive, focusing on identifying and addressing risks only after they have materialized. This delayed response can result in significant financial and reputational damage.

The need for a paradigm shift: Introducing Quantifind Payments Risk Intelligence

Quantifind Payments Risk Intelligence is an advanced method that leverages purpose-built artificial intelligence (AI) and machine learning (ML) to provide a comprehensive and holistic risk analysis approach that spans pre-, during, and post-alert generation. Unlike traditional transaction monitoring, which primarily focuses on flagging transactions based on static rules, Quantifind Payments Risk Intelligence analyzes customer and counterparty behavior and relationships at the pre-alert generation phase at scale and with unprecedented speed and accuracy.

The Benefits of Precise Language Models

Traditional transaction monitoring systems rely on static, predefined rules to flag suspicious transactions. These rules are rigid and do not adapt to changing financial crime patterns. As a result, they often fail to detect new and evolving threats, leading to higher false positive and false negative rates. The inflexibility of static rules makes it difficult to keep up with the dynamic nature of financial crimes. This is similar to a keyword-based approach to adverse media screening, where reliance on a static list of keywords (e.g., “fraud,” “arrest”) can lead to missed critical context if terms like “misappropriation” are not included.

In contrast, precise language models powered by artificial intelligence offer a more sophisticated approach. These models can analyze large datasets, understand complex patterns, and adapt to new data inputs. They provide higher accuracy in detecting true financial crimes while reducing false positives. AI-driven systems are dynamic and can continuously learn and improve, making them more effective at handling the complexities of modern financial crimes. Additionally, they operate much faster and can scale efficiently to handle large volumes of transactions.

Due to the exploding scale of payments, precise language model solutions must offer scalability and accuracy. A foundation language model with over 100 billion features would be orders of magnitude too slow to process high-volume payments. Therefore, a separation between model build and model runtime is required, where predictive features are learned on a massive language model but then implemented in a much more compact model for large-scale enterprise throughput. These reduced-dimensional models are also more transparent and explainable to regulators.

Quantifind uses this advanced approach to assess payment counterparty risk, utilizing transaction information and vast open-source information from news articles, regulatory enforcement actions, and company intelligence data. This method reverses the traditional problem-solving approach by focusing on external risks as triggers, allowing investigators to align these with transaction patterns and take appropriate actions. With configuration knobs to tune the model according to the risk tolerance of the financial institution, the alerts produced are designed to be both precise and relevant, significantly reducing irrelevant findings and enhancing the prevalence of material discoveries.

Key Benefits

Find hidden risks with speed and accuracy—
precise language models combined with proprietary name science and best-in-class entity resolution ensure accurate, actionable risks are identified.

Scale your analytics to a limitless number of entities and their counterparties—
flexible architecture and highly performant implementation scales with the business, ensuring you never fall behind.

Get a holistic view of entity risk—
enrich all payment parties and counterparties with a holistic risk assessment based on information inside and outside the financial institution.

Customize the solution to
align your risk appetite with the implementation and only review the most relevant alerts.

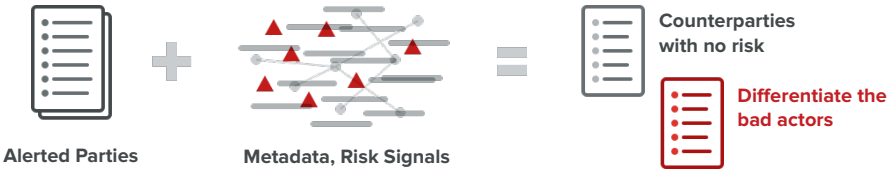
The Quantifind Payments Risk Intelligence Approach

1. Intelligence-driven Counterparty Risk Analysis

Pre-Alert Generation | Alert Generation | Post-Alert Generation

Risk intelligence on transaction counterparties:

- Upfront screening and identification of counterparties based on underlying characteristics (DOB, address, registration, etc.)
- Extraction of risk signals on underlying counterparties differentiating good vs. bad actors



Benefits:

- Faster counterparty research/ investigation
- Risk-based investigation due to upfront knowledge about underlying counterparty risks
- Identification of potential false positives based on counterparty risk

Effort considerations / preconditions / challenges:

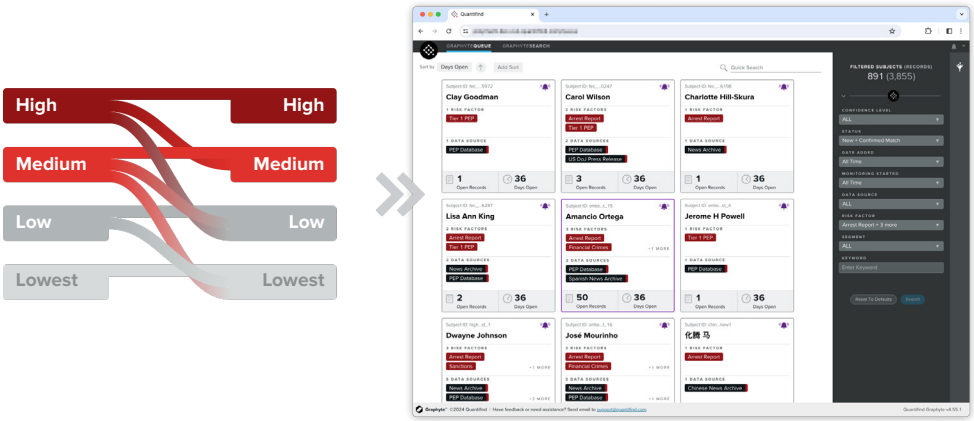
- Access to transaction and counterparty data
- Availability of analytics infrastructure
- Counterparty risk is not representative of the entire alert risk

2. Automated Risk-based Prioritization and Workflow Optimization

Pre-Alert Generation | **Alert Generation** | **Post-Alert Generation**

Alert risk scoring and prioritization:

- Augment Quantifind's risk signals with transaction analysis and apply AI-based scoring model to classify and score alerts based on risk profile of underlying transaction activity
- Prioritize alerts based on risk score and segment into high, medium, low, lower (potential false positive)
- Automatically route alerts based on risk-based workflows and team specializations (e.g., Prior SAR highest alerts to a specific team)



Benefits:

- Accelerated review of riskier alerts
- Potential auto-closures based on risk classification and automated research

Effort considerations / preconditions / challenges:

- Testing/Training data availability for accurate alert classification
- Alignment with procedures to define automated actions, especially concerning lowest risk potential false positives
- Iterative collaboration with client SME to refine parameters and review outcomes

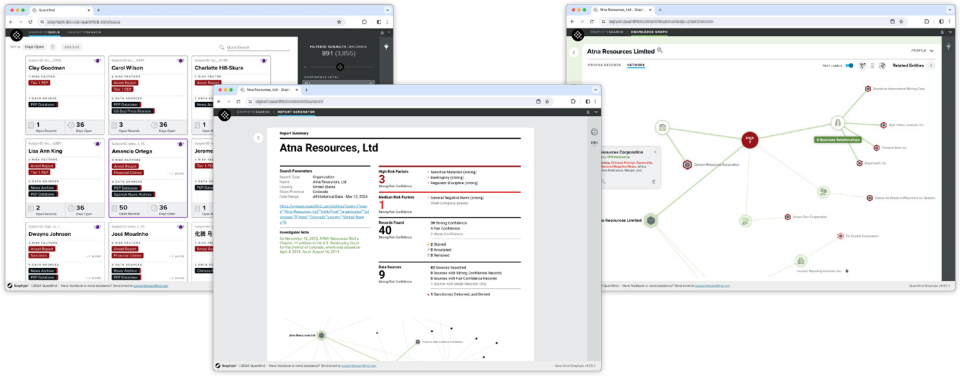
3. Streamlined Alert Insights

Pre-Alert Generation | Alert Generation | **Post-Alert Generation**

Automated alert risk factor summarization:

- Summarizes risk signals and underlying alert characteristics and explains the risk score
- Enables quick understanding of the risk score rationale and additional critical details about the alert at a glance





Benefits:

- Reduces time spent analyzing risk factors
- Easily ingestible alert characteristics and risk score explanation
- Readily available summarized counterparty research

Effort considerations / preconditions / challenges:

- Customization to include or emphasize certain data points
- Iterative collaboration with client SME to define feature review summaries
- Access to underlying transactional data and infrastructure for LLM models to generate summaries

4. Narrative Generation

Pre-Alert Generation | Alert Generation | **Post-Alert Generation**

Automated alert/SAR narrative generation:

- Summarizes alert metadata, transaction activity, counterparty risk, investigator inputs, and related alert dispositions
- Drafts a comprehensive narrative using LLMs for alert closure and SAR escalation



Benefits:

- Faster alert closure with automated narratives
- Expedites and simplifies QC
- Reduces human error

How to Assess Your Technology Choices

New Criteria	Traditional Transaction Monitoring Solutions	Quantifind Payments Risk Intelligence
Uncovering Hidden Risks in Customer Relationships	Does not analyze the customer network of connections at scale and with speed and accuracy.	Goes beyond mere transaction monitoring by examining the relationships and behaviors of customers through network discovery.
Scaling Risk Analysis to Billions of Customers and Their Connections	Scale is constrained by manual processes the inability to handle high data volumes, and increased processing power.	Unlimited ability to scale to your needs.
Accuracy of Risk Detection, thereby Reducing false positives	Limited data coverage, antiquated AI models, and manual processes produce a high volume of false positives and false negatives.	Proven, purpose-built AI models detect true risks with high accuracy.
Speed of Quality Risk Discovery	Provides speed but at the expense of low-quality results.	Offers rapid and high-quality risk discovery through advanced AI and ML techniques.
Report True Financial Crime vs. Meet a SAR Quota	A defensive approach to compliance is needed due to accuracy, speed, and scale issues.	Enables proactive reporting of true financial crime by ensuring precise, timely, and scalable risk detection.
A Comprehensive view of customer behavior	Customer intelligence is limited to their transaction behavior. The aggregation of customer intelligence is often manual.	Quantifind integrates data from multiple sources, offering a holistic view of potential risks. This integration enables more consistent and thorough risk assessments, enhancing the organization's protective measures.

Public and Private Partnerships to Define Risk Cards

Public and private partnerships are crucial in the fight against financial crimes, particularly in supporting conservationist movements and ensuring the safety of our planet. These collaborations leverage the strengths and resources of both sectors to address complex challenges that neither could tackle alone. Public entities provide regulatory frameworks, enforcement capabilities, and access to critical intelligence, while private organizations contribute innovative technologies, data analytics, and financial resources.

At Quantifind, bridging sectors is part of our company strategy. Our contribution facilitates collective discussion through a Convergence program and walks the talk through a one-of-a-kind Risk Card initiative. Risk Cards are a vehicle to facilitate collaboration between domain experts, data scientists, and information consumers to create models that comprehensively identify signals and assess the relevance of those risks. These cards help “scale expertise” by operationally defining each risk and setting machine learning models up for measurable success and validation. Furthermore, the approach goes a long way toward establishing a transparent, responsible approach to AI by clearly documenting the model’s risk-targeted definitions. Taking the taxonomy and documentation another step further, integrating this risk schema with a comprehensive knowledge graph that fuses information from many open source intelligence (OSINT) data sets, Quantifind hopes to help partners map and disrupt wildlife trafficking networks across the globe.

Together, public and private partnerships help to enhance the detection and prevention of financial crimes that threaten conservation efforts, such as illegal wildlife trafficking, human trafficking, and environmental exploitation. By working in tandem, public and private sectors can create more robust, comprehensive strategies that protect biodiversity, preserve natural habitats, and promote sustainable development, ensuring a safer, healthier planet for future generations.

Conclusion

A holistic AI approach to payments risk management addresses the challenge of massive payment scale by assessing the lifecycle from the first client touchpoint through the transaction. This changes the philosophy from reactive anomaly alerting to a proactive understanding of the risk of counterparties, automated network analysis, and a technology commitment to workflow optimization and installing automated steps efficiently and thoughtfully. In an era where financial crimes are becoming increasingly sophisticated and pervasive, it is clear that traditional payment risk management methods are no longer sufficient. The flaws of high false positives, missing genuine threats, and process inefficiencies hinder the ability of financial institutions to combat financial crimes effectively. The need for a paradigm shift to advanced payments risk intelligence is not just a strategic advantage but a critical necessity to discover the hidden criminal threats to a payment system - while simultaneously providing operational cost savings.

Scan this QR code to visit us at www.quantifind.com Reach us: salesteam@quantifind.com

© Copyright 2024. Quantifind’s precise risk intelligence automation empowers organizations to investigate entities, and uncover relevant risk signals with supreme accuracy, speed, and scale. Quantifind‘s AI platform, Graphyte, streamlines risk management workflows by delivering superior entity resolution, dynamic risk typologies, and advanced knowledge graph technology and name science. Join the tier one institutions that are benefiting from better results.