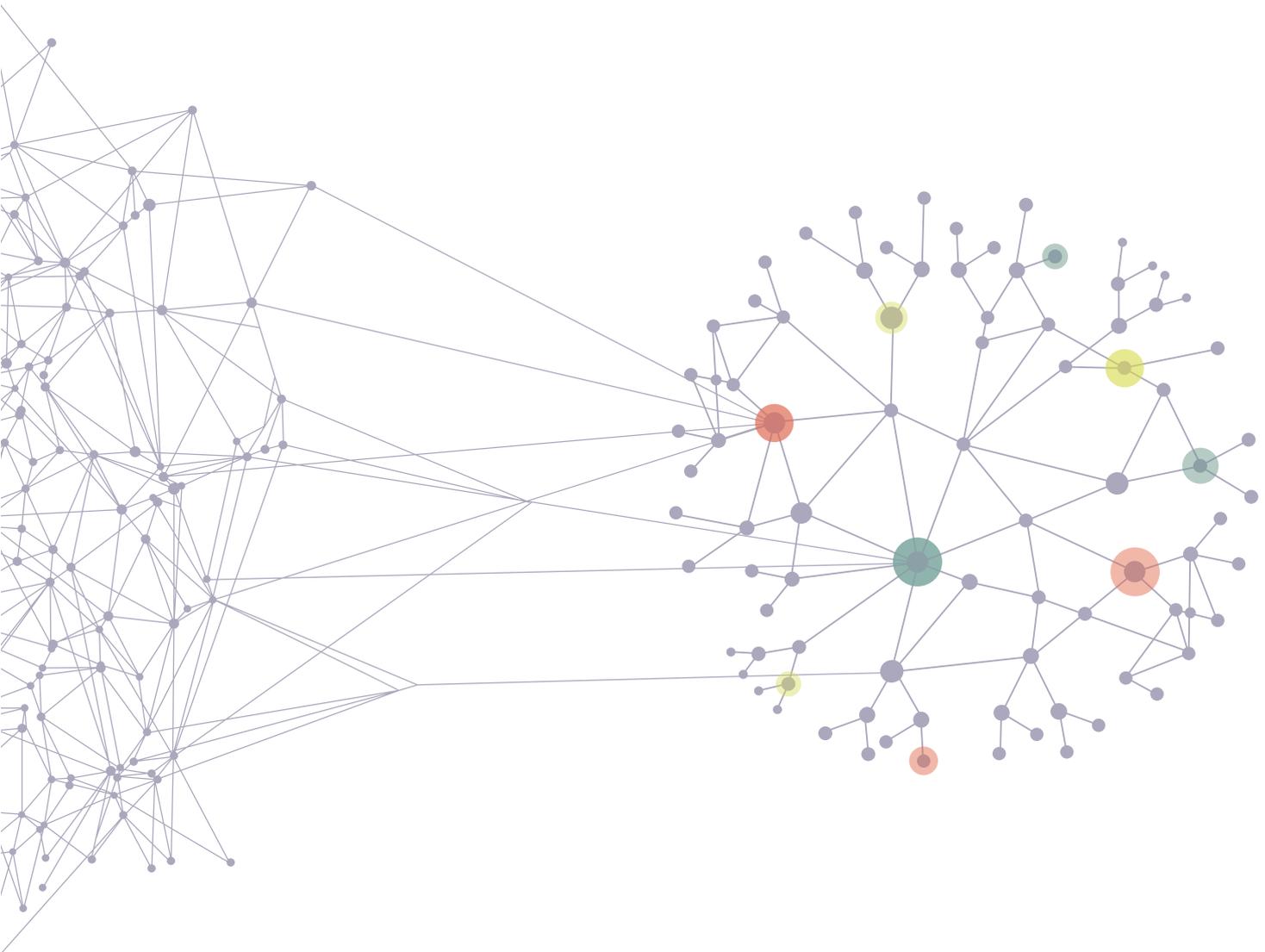




Contextual Monitoring: A New Approach to Markets Transaction Monitoring



Executive Summary

Leading global banks are reassessing the Anti Money Laundering (AML) systems that protect their Markets business. Many systems and processes used today were rapidly deployed in response to regulatory pressures, but don't provide the latest, most relevant approaches to Markets AML.

Banks are therefore often heavily reliant on non-Market specific detection models, such as those repurposed from retail banking AML, or market abuse monitoring. These models are used in conjunction with manual supporting processes that try and address Market specific needs. This has led to an overall lack of effectiveness and rising costs due to inefficiency.

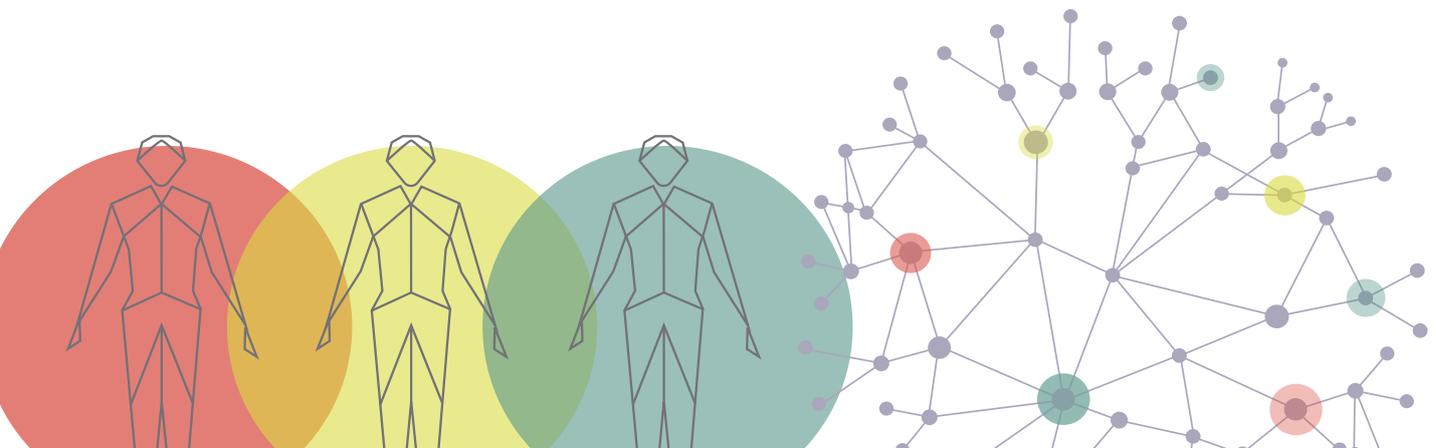
The new best practice is *contextual monitoring*, which addresses the fundamental issues of traditional rule based transaction monitoring approaches. *Contextual monitoring* foundationally uses entity and network analytical techniques, in combination with advanced analytical methods, such as behavioral and peer group analysis, to detect anomalous and suspect activity.

Deploying *contextual monitoring* creates an adaptable and scalable approach that allows a bank to understand all that is reasonable to know about their Markets clients at a given point in time, including their past historical activity and relevant relationships.

The *contextual monitoring* approach provides increased:

- **Coverage** of clients and segments;
- **Effectiveness** in alerting suspect behavior;
- **Efficiencies** in completing investigations; and
- **Agility** to adapt and detect to new behaviors.

This paper discusses the *contextual monitoring* approach and details the best practice methodology.



The need for a new approach

The Markets business has the potential to house complex money laundering behaviors and banks have difficulty defining their AML transaction monitoring requirements in this space. Many banks rely heavily on manual processes and reviews to identify suspect activity, and those that have systems in place, have attempted to adapt retail models or market abuse models. Typically, such systems are pre-configured and off-the-shelf scenarios are used, leading to ineffective output and inefficient systems.

Challenges to banks within Markets AML include:

High levels of low quality alerts:

- Basic detection methods are used (e.g. rules and entry level anomaly analysis);
- Monitoring occurs at a transaction (trade or settlement) or account level in isolation;
- Available data is not used in all instances; the focus to date has been on third party payments and the source of funds for such payments; and
- Systems are unable to deal with poor quality or inconsistent data.

Poor coverage:

- Little or no bespoke tuning to the products or scenarios to be monitored;
- Limited scenarios in place; and
- As a result, single digit SARs filed, many of which originated outside the monitoring system.

Lack of system flexibility and transparency:

- Systems are inflexible and unable to support the addition of new products, data points and typologies; and
- Analytical processes, if present, are hidden and cannot be reconfigured easily. This results in degradation of model performance.

Workarounds:

- Difficult to manage and support, workarounds are often implemented in a non-strategic manner through technical teams writing bespoke code.

Many money laundering behaviors will not be detected by looking at transactional or account activity in isolation; they will involve a complex web of behaviors, companies, individuals, trades, settlements, and payments.

This drives the need for a methodology that can provide a more holistic approach to monitoring; one that is able to risk assess all entities and networks of connected parties and behaviors. This new approach provides an aggregated view of risk across all the available data, as well as utilizing sophisticated behavioral analytical techniques to understand normal versus abnormal behavior.

Contextual Monitoring

By generating low volumes of higher interest alerts, *contextual monitoring* provides gains in AML effectiveness and efficiencies in the Markets business. *Contextual monitoring* uses big data techniques and advanced analytic capabilities to detect anomalous behavior, accounting for all that it is reasonable to know about a client or counterparty at a given time. In effect, it replicates the laborious parts of investigative process, but does so in an automated, yet fully transparent and understandable manner. This frees up analyst time to concentrate on the investigative aspects of the alert. In addition, the wider data sets involved give the analysts earlier sight of the potential full extent of the case they are currently investigating.

The end result is a process that offers the following benefits:

Greater accuracy and improved effectiveness, reducing false positives and finding more potentially high-risk activity. This is achieved by:

- Wider use of available data as part of a risk assessment, including using improved company and KYC data, as well as 3rd party sources to fully understand company structures;
- Extensive use of analytical methods such as behavioral analytics, peer group analysis and anomaly based detection to provide a greater assessment of normal versus abnormal; and
- Use of dynamic entity and network based techniques, so that activity can be risk assessed holistically across connected companies and related activity.

Improved coverage through:

- More extensive scenario implementation;
- Ability to easily adapt to cover new scenarios as they emerge – including extension of the underlying data fed into the system, as well as new analytical techniques and output.

Furthermore, a contextual approach naturally capitalizes on the big data and open analytics strategies that banks are heavily invested in. This results in: far less data replication; re-use of existing security models; and an open and extensible architecture.

By combining transactional based monitoring with holistic behavioral monitoring, the contextual approach identifies both specific instances of suspect client behaviors and longer-term client behavioral changes. This immediate and long-term monitoring approach aligns with banks continuous Customer Due Diligence (CDD) programs.



Method Overview

Contextual monitoring generates low volumes of high quality alerts that are specific and relevant to the Markets products being monitored. The automated alerting approach follows four steps, each of which feeds into the next:

1. **Acquisition** of relevant internal and external data
2. **Enrichment** of data to produce a holistic client view
3. **Scenario application** using multiple analytical techniques
4. **Alert generation** with relevant context, that identifies specific risks

Identifying relevant data

If a data source can contribute towards a clearer understanding of who a client is, who they are connected to, or how they behave, then the data source is considered relevant for contextual monitoring.

These relevant data sources can be split into two categories based on their typical frequency of update:

- **Static or slowly changing data** such as data records originating from Know Your Client (KYC), Enhanced Due Diligence (EDD), Customer Risk Rating (CRR) and third party/external sources such as Ultimate Beneficial Ownership (UBO) information. These records, following later enrichment, will ultimately contribute to a better understanding of the client's type or categorization, and further provide factual linking information. For example, factual links may be automatically identified through common addresses, companies or directors that reveal who and what the client is directly and indirectly associated with.
- **Behavioral data** such as data records originating from trade, settlement, payment, transfer, and account operation systems. These records, following later enrichment, will ultimately contribute to a better understanding of how the client operates their accounts, the recency, frequency and monetary values (RFM) of their deposits and trades, and the channels through which they settle. In addition, behavioral links may be automatically identified such as links to the accounts, people, organizations, and countries that funds are received from and settle to, again revealing who and what a client is directly and indirectly associated with.

For contextual monitoring, the static and slowly changing data sources should be ingested regularly as they become available. The behavioral data sources, including transactions related to trades and settlements, represent a continuous, high volume stream and hence a filtering and/or pre-aggregation step is recommended to identify the records that will provide the most relevant behavioral and linking information. Such records should then be ingested into the contextual monitoring system.

Enriching the relevant data

Following acquisition of relevant data, automatic enrichment then provides a holistic view of each client from all the data and provides the base context from which monitoring will then take place.

Key enrichment outputs include:

- **Behavioral profile** – building up the behavioral profile for each client, based on their account operations and all relevant details of their trade instructions.
- **Entities and matching** – resolving entities to identify every true, single person, place or organization that may be represented in many disparate records from different sources with non-matching record IDs.
- **Segmentations** – identifying multiple relevant segmentations for the ultimate purpose of defining relevant peer groups. Segmentations can be static such as geography, client type, industry type or dynamic/behavioral such as funding and settlement channels, trading RFM etc. Note, the segmentations are not intended to be the same as existing customer risk rating based segmentations, but rather are for analytical peer group identification.
- **Relationships** – identifying relevant, direct links and connections the client has to other clients, people, places and organizations (entities), through internal and third-party data sources.
- **Network profile** – moving beyond direct relationships from one client and instead to identifying indirect relationships to multiple other clients and entities.

Scenario based detection

Analysing each trade or event in isolation generates significant noise and does not give a true picture of an overall risk faced. Therefore, the contextual approach uses the enriched data as the basis upon which scenario-based, risk detection is applied. Scenarios include a range of approaches and analytical techniques and the scenarios will ultimately be aggregated together to form an overall, composite score.

Scenarios are applied across all relevant levels, i.e. at the trade or account level, the client level, and where applicable, the network level. Scenarios include:

- **Business Rules** that automatically encode many core investigative questions that an investigator would repeatedly seek to answer.
- **Behavioral Risk Indicators** specifically relevant to the Markets products being monitored, that represent individual risk components that can be later combined to identify specific risks.
- **Anomaly Detection** based on a client's account usage or trading behaviors compared to previous client behavior.
- **Peer Group Analysis** to further compare client's behavior to a baseline from relevant peers, to further clarify if a behavior is indeed unexpected.
- **Trained Models** using the most appropriate analytical techniques at the point when training data becomes sufficiently available.

Figure 1 illustrates several key scenario approaches, including Behavioral Risk Indicators, Anomaly Detection, and Peer Group Analysis, all of which are applied to an enriched view of a Markets client that contains both static and behavioral segmentations and segments.

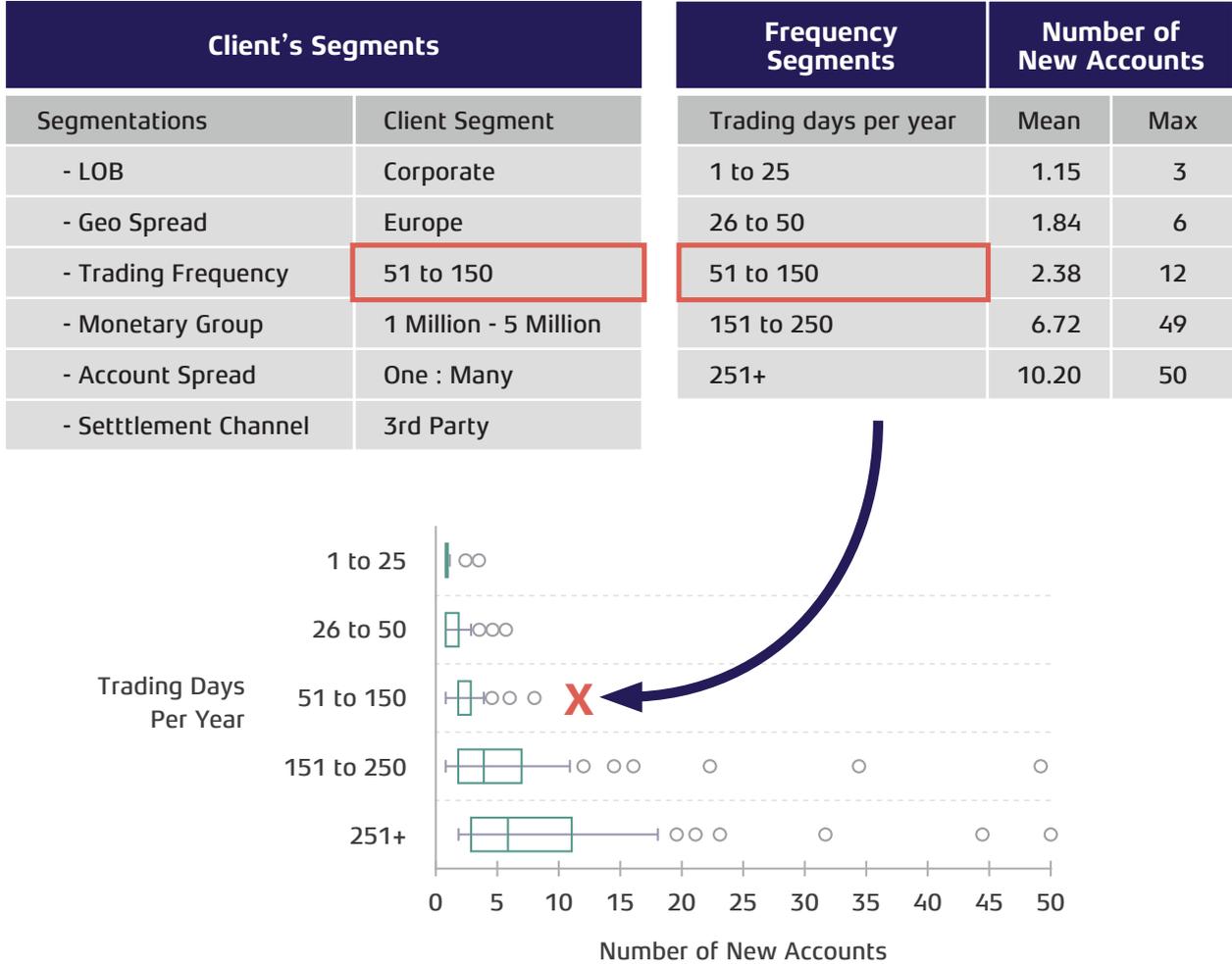
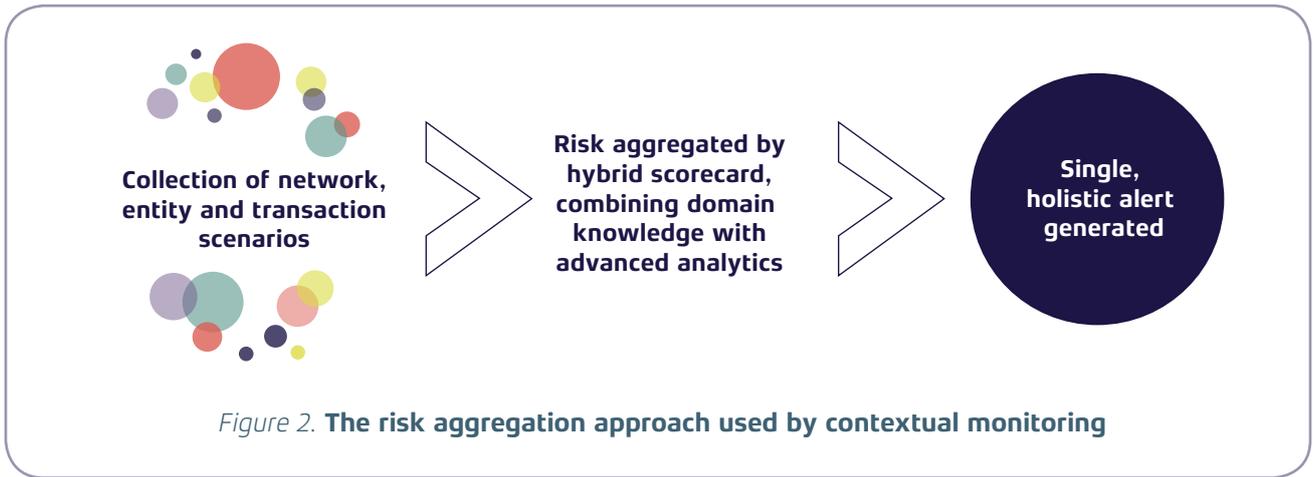


Figure 1. This example shows a Market client with a modest trading frequency (an average of 1 trade per week), but who has an account usage that resembles clients who trade multiple times a day. This anomaly is used in combination with other scenarios as a risk factor for trades to recently opened accounts.



Alert Generation

Following the application of scenarios to the enriched data, the final step is to generate contextual alerts. Each alert is an aggregation, where a specific composite model combines lower level components. This approach takes into consideration all available aspects of behavior, i.e. the wider context, and does not just trigger an alert based on a single rule or event. An overview of this approach is shown Figure 2.



The aggregation approach is further illustrated in Figure 3 by an example alert from FX based trade/settlement monitoring.

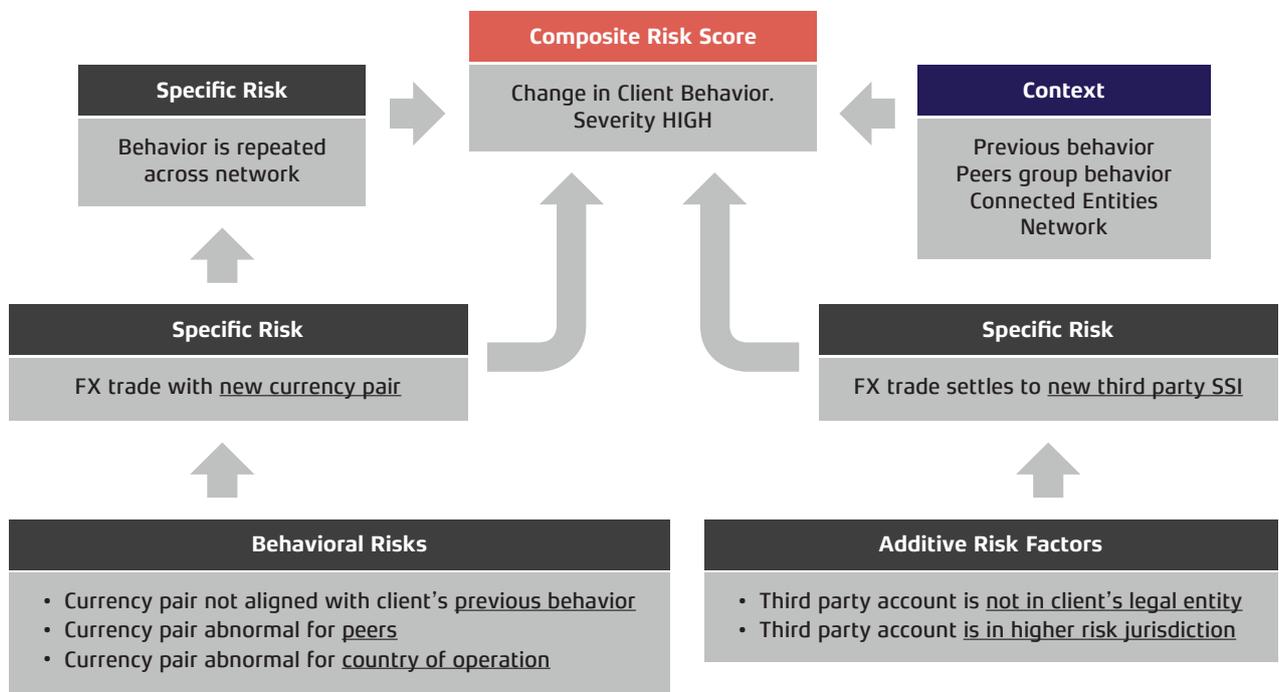
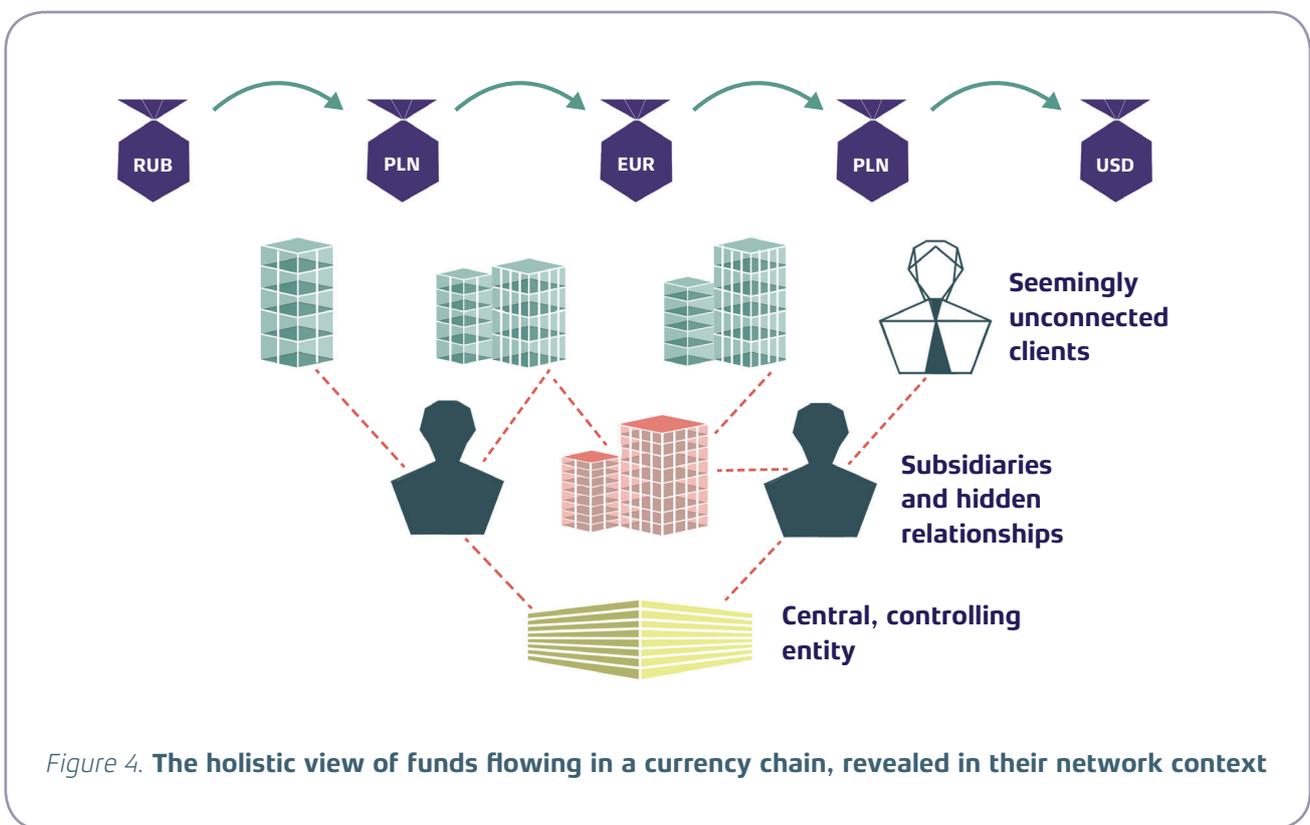


Figure 3. An example FX trade/settlement alert that uses a model to aggregate components together to create a Composite Risk Score.

Context

The high accuracy of alerts is achieved through the automatic consideration of the Markets clients' behavior *within its true context*. This context includes a combination of: the client's previous behavior; their peer group's behavior; their relationships; and their network behavior.

An illustration of a network context is shown below. Here we identify the unusual flow of funds forming a currency chain. A series of buy and sell trades occurs between seemingly unconnected clients, which in itself is not suspect. However, the currency is cycled in a short period of time and the overall picture shows higher risk countries and currencies being utilized. The holistic picture reveals that a central controlling entity is using lower risk subsidiaries and currencies to facilitate money laundering through the chain.



Conclusion

The lack of accurate, automated monitoring leaves Markets vulnerable to money laundering activity. Global banks are instigating new initiatives with the next generation of *contextual monitoring* capability. *Contextual monitoring* reveals the wider context surrounding a client's activity, offering a holistic assessment of the money laundering risk they pose.

Contextual monitoring requires entity resolution, network generation and behavioral analytics, making use of rich behavioral and linking data available internally and externally. Importantly, these new initiatives align with the bank's analytics strategy by providing open platforms that make use of existing big data architecture, analytics initiatives and available skills.

The benefit of this approach is enhanced monitoring; monitoring that is effective at finding high-risk activity with an acceptable level of false positives. Additionally, it offers a greater efficiency and wider coverage of the more pressing money laundering risks, by presenting the big picture, pre-assembled and ready for investigation.



quantexa

T +44 2031 372 533

E info@quantexa.com

Quantexa, Three Tuns House,
109 Borough High Street,
London SE1 1NL