# NICE Actimize

eBook

Understanding Counterparty Risk in Correspondent Banking

NICE Actimize

Overview of Correspondent Banking

Correspondent banking poses a significant risk when it comes to ensuring respondent banks are conducting the proper anti-money laundering (AML) checks and have implemented the appropriate controls. Correspondent banks must conduct Enhanced Due Diligence (EDD) on their respondent banks and maintain a thorough and up-to-date risk assessment to help manage and mitigate risks posed by these services.

NICE Actimize
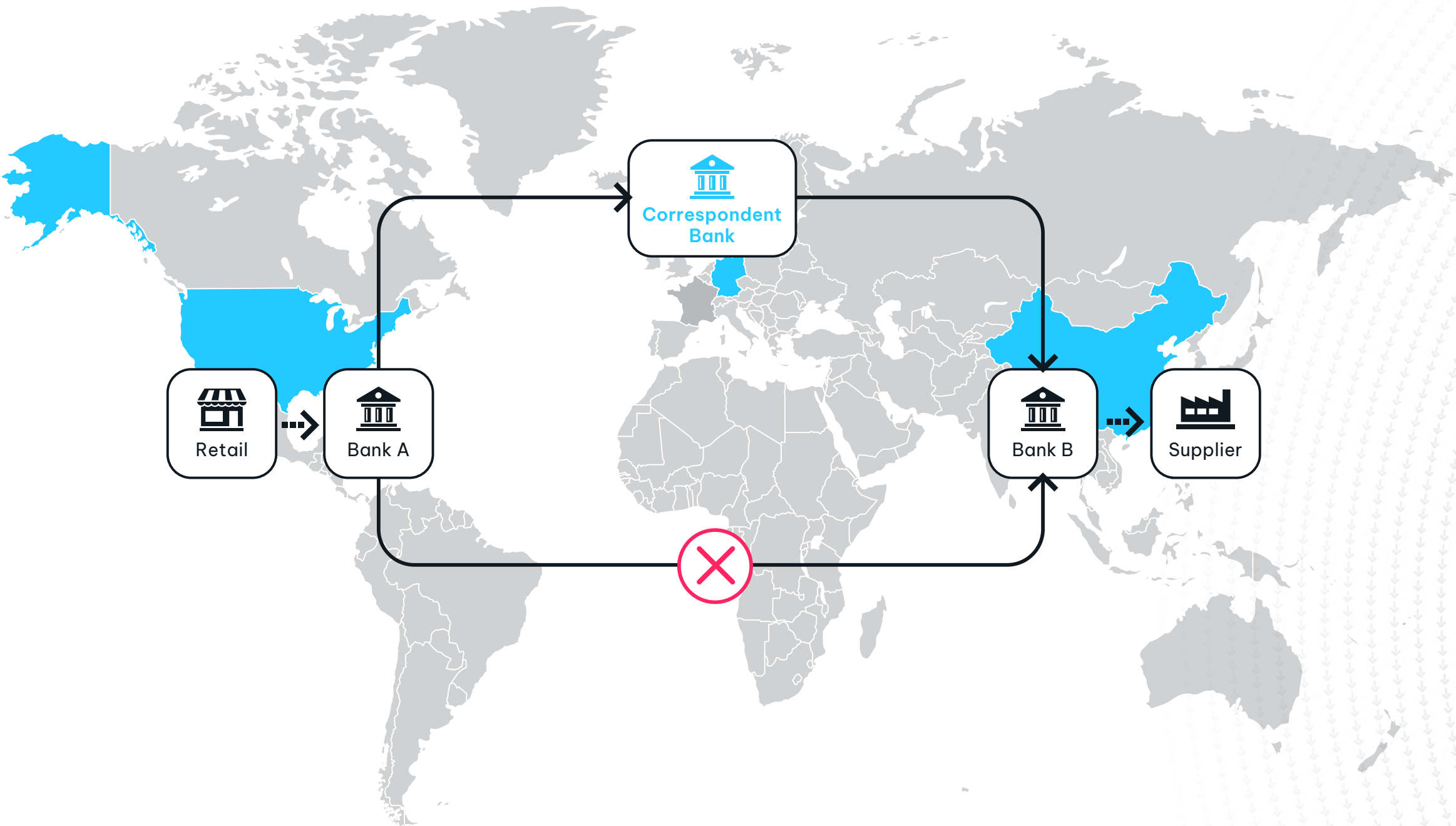
What is Counterparty Risk in Correspondent Banking?

Counterparty risk, also referred to as third-party risk or pseudo-client risk, is a serious concern for correspondent banks. Correspondent banks are required to conduct enhanced due diligence on their customers, the respondent bank. They are not required to perform due diligence on the respondent banks' customers, increasing exposure to potential financial crime risk.

Correspondent banks rely on respondent banks to have effective financial crime compliance controls, policies and procedures, and adequate monitoring both across Know Your Customer (KYC) and transaction monitoring. Putting their trust in respondent banks to conduct effective due diligence, transaction monitoring, and other AML measures is the true risk to correspondent banks. Controls can vary considerably depending on the respondent bank, which can leave correspondent banks exposed to gaps or weaknesses.

NICE Actimize
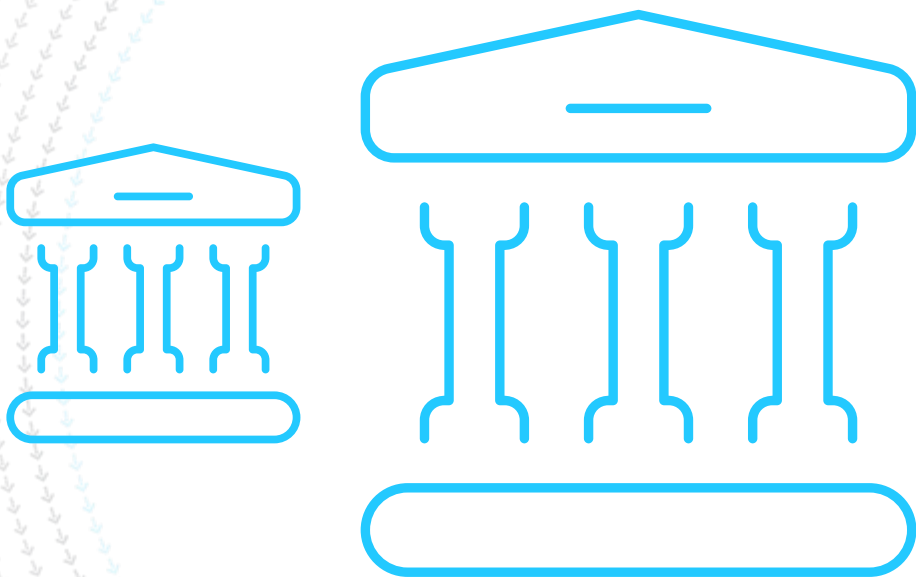
Challenges in Understanding Counterparties

Due to the many complexities presented by counterparties, these are the top challenges correspondent banks are exposed to:

Lack of Information on Counterparties
Lack of KYC information on originator or beneficiaries makes it much more difficult to resolve counterparties as an intermediary.

No Control Over Originating Customer
Because transactions originate from a third party, correspondent banks have no control over respondent banks or those customer transactions.

Complex Network Structures
With limited access to information, it's hard to identify the rational for transactions and connections between counterparties, so understanding if the flow of funds is legitimate or arduous.

Indirect Structure
Some financial institutions (FIs) act as aggregators for smaller ones. This is known as nested banking. These structures can be complex and opaque, which can increase the correspondent bank's risk.

Geographic Diversification
Correspondent banking relationships span multiple countries, each with distinct regulatory requirements and varying levels of AML compliance. This adds additional complexity to risk assessments.

Emerging Payment Methods and Digitization
The use of emerging payment methods, such as cryptocurrencies and digital wallets, can complicate monitoring and understanding counterparties and their risks.

NICE Actimize

Typical Risks Presented by Counterparties

There are a variety of threats involved with counterparty risks, here are just a few:

Money Laundering
Counterparties may engage in money laundering, disguising the illicit origins of funds and facilitating the movement of illegal money across borders.

Terrorist Financing
Correspondent banks could unknowingly or intentionally facilitate funds for terrorist organizations or individuals.

Fraudulent Activity
Counterparties may be involved in fraudulent schemes, impacting not only FIs, but also consumers and other businesses.
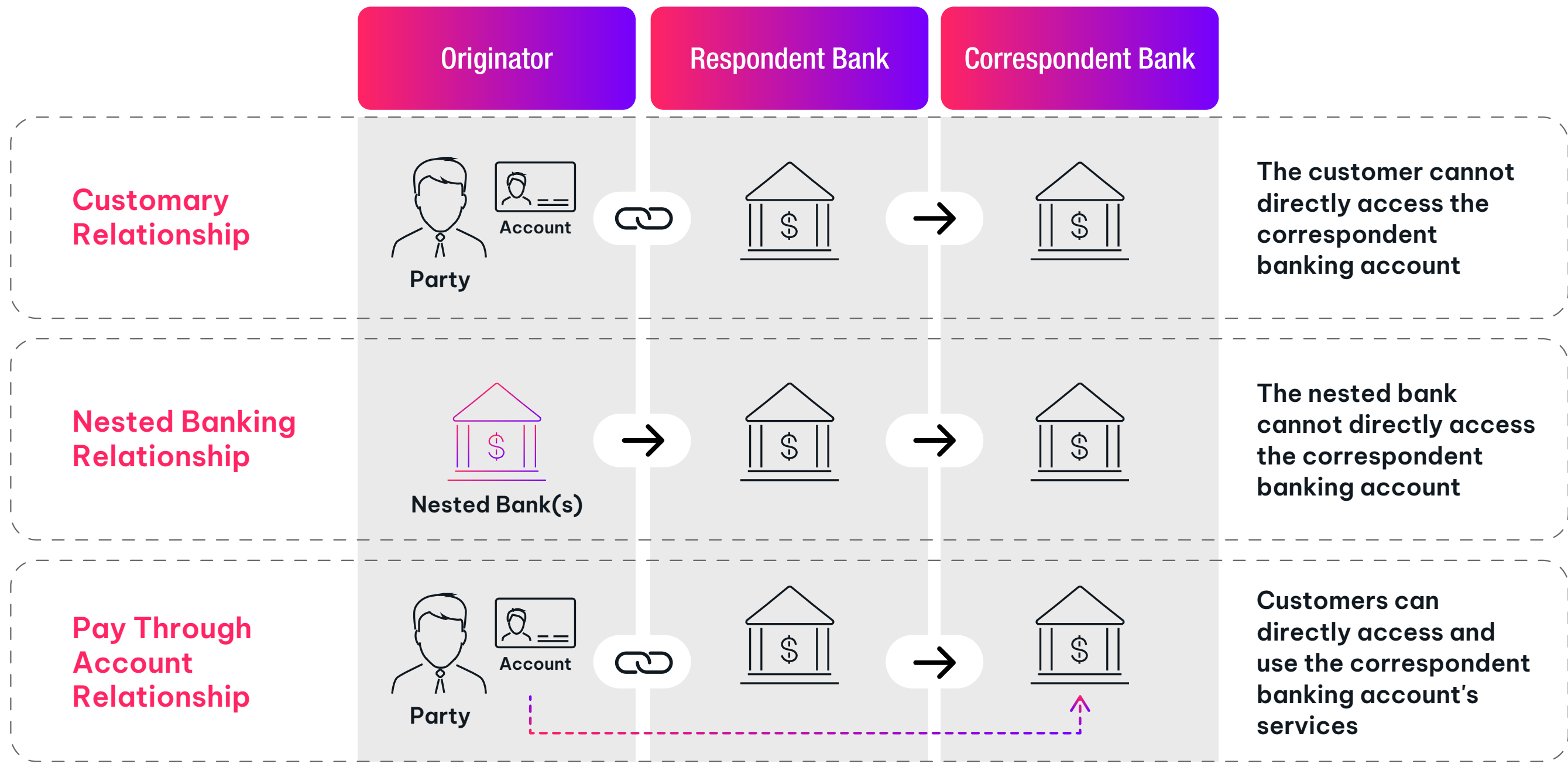
Sanctions Violations
Correspondent banks can inadvertently deal with counterparties that are sanctioned, leading to regulatory and reputational risks.

Regulatory Non-Compliance
Respondent banks' failure to comply with AML regulations or their poor financial crime controls can result in legal and regulatory actions, directly impacting correspondent banks doing business with them.

NICE Actimize

High-Risk Counterparty Relationships

Some respondent banks have higher-risk relationships, which present additional risks to correspondent banks when facilitating payments. These relationships can have less transparent payment structures; it's much more difficult for correspondent banks to determine the originators, beneficiaries, and parties involved in each transaction.

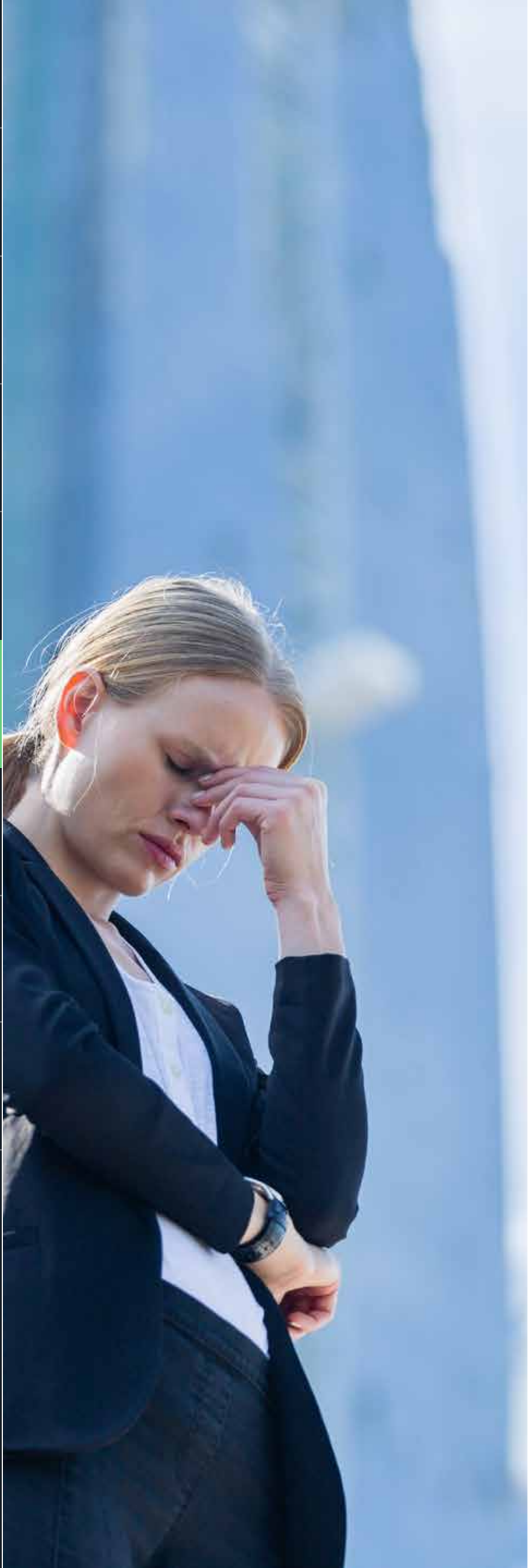|	Originator	Respondent Bank	Correspondent Bank	
Customary Relationship	Party / Account	Bank	Bank	The customer cannot directly access the correspondent banking account
Nested Banking Relationship	Nested Bank(s)	Bank	Bank	The nested bank cannot directly access the correspondent banking account
Pay Through Account Relationship	Party / Account	Bank	Bank	Customers can directly access and use the correspondent banking account's services

NICE Actimize

Correspondent banks call accounts held at their institution by a respondent bank a Vostro account. Respondent banks refer to these same accounts that they hold at a correspondent bank as a Nostro account. Nostro and Vostro are derived from the Latin for "ours" and "yours," respectively.

High-Risk Counterparty Relationships

Nested correspondent banking

The use of correspondent banking services by several indirect respondent banks (nested banks) through the direct respondent bank.

Pay through accounts

Pay through, or pass-through, accounts that can directly access the Vostro account, allowing the end customer to conduct transactions through this account.

With complex financial interactions, potentially involving multiple correspondent/respondent banks, FIs can inadvertently expose themselves by providing services to extremely high risk or prohibited entities, including:

Shell corporations

Corporations without significant assets or active business operations that have the potential to be used for illicit activities, such as layering financial transactions to conceal the source of funds and the identity of parties involved.

Shell banks

Banks without a physical presence within the incorporated/licensed country and unaffiliated with a regulated financial group. Because shell banks don't have a physical presence, a supervisor in the licensing jurisdiction cannot regulate these banks. U.S. banks are prohibited from establishing, maintaining, administering, or managing accounts for foreign shell banks.

NICE Actimize

Negative Impact on Business

Not managing correspondent banking risk effectively can result in:

Reputational Risk

Failure to effectively understand and mitigate the risks posed by counterparties can lead to reputational damage, attracting unwanted media attention, and eroding trust with clients and regulators.

Regulatory Scrutiny

Inadequate understanding and management of counterparties can result in regulatory fines and enforcement actions, harming the bank's financial health.

Operational Costs

Potential fines, protracted legal disputes, and the increased resource allocation to mitigate damages can have a profound impact on an FI's financial performance. Additionally, the distraction posed by such proceedings may impede operational efficiency, affecting profitability.

Business Disruption

The discovery of high-risk counterparties may lead to business disruptions, including the termination of correspondent relationships, impacting revenue streams. In specific regions, it can cut off adequate access to the international financial system.

NICE Actimize

Benefits of Optimizing AML Strategies

Greater understanding of respondent banks and underlying customer activity through consolidated and enriched data, combined with the right technology, improves risk assessment, and identification of suspicious activity.

A few of the benefits include:

Robust Entity Profiling

Boost cross-border payment risk assessment for correspondent banks with AI-based entity profiling, eliminating duplicates, and linking involved entities for accurate risk profiles.

Enhanced Suspicious Activity Detection

Improved counterparty risk knowledge enhances transaction monitoring, allowing banks to better detect and expose potential money laundering through identification of unusual activities.

Understand Correspondent Networks and Relationships

Deep counterparty risk understanding enables crucial network analysis, unveiling hidden connections among counterparties, originators, intermediaries, and beneficiaries to identify complex money laundering schemes and bad actors.

Precise Reporting and Data Visualization

Thorough risk assessments facilitate accurate regulatory reporting. Dashboards visualize operational data, ensuring compliance, mitigating regulatory risk, and preventing penalties.

Efficient Resource Allocation

Efficiently allocate compliance resources based on counterparties' risk levels, reducing operational burden and maintaining rigorous AML standards.

NICE Actimize

A New Approach to AML

Traditional AML practices for correspondent banking often leaves FIs in the dark about their customers' customers, exposing them to elevated risks. Regulatory expectations have grown more stringent, necessitating an innovative technology-driven approach to bolster AML efforts. Advanced technology solutions offer correspondent banks the means to gain a more comprehensive insight into counterparty risk, enabling them to reduce financial crime risk without having to resort to de-risking.

These solutions leverage data analytics, AI, and machine learning (ML) to streamline processes, provide comprehensive risk monitoring, and deliver actionable insights to mitigate financial crime risks effectively. For correspondent banks to remain compliant and profitable while maintaining valuable correspondent banking relationships, innovative technology solutions are essential.
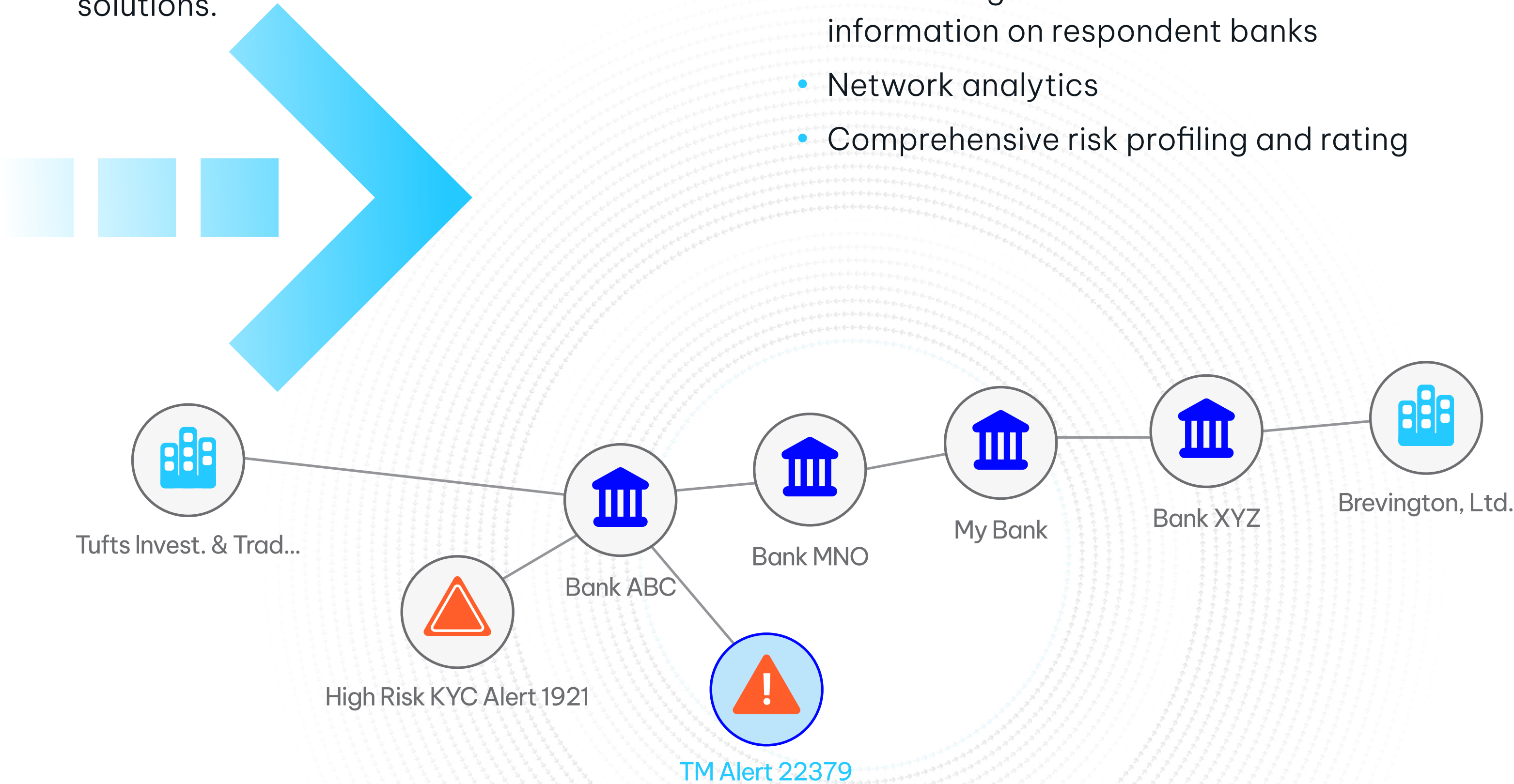
NICE Actimize
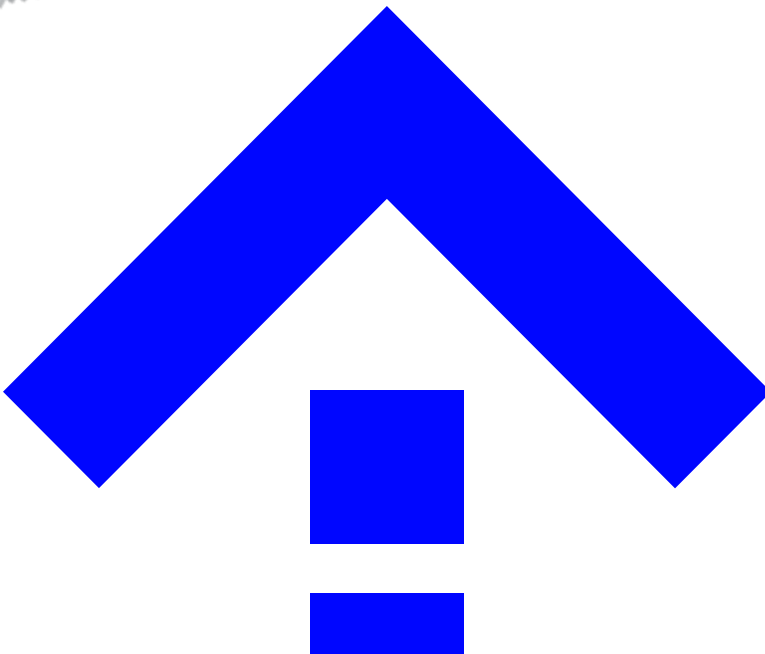
Streamline Respondent Banking KYC

Correspondent banks can streamline their KYC process and improve risk rating and risk management for new respondent banks using AI-powered solutions.

Ensure an extensive understanding of your respondent bank customers with:

- Data intelligence tools to enrich known information on respondent banks
- Network analytics
- Comprehensive risk profiling and rating

Tufts Invest. & Trad...

High Risk KYC Alert 1921

Bank ABC

Bank MNO

My Bank

Bank XYZ

Brevington, Ltd.

TM Alert 22379

NICE Actimize

Advanced Analytics for Pinpoint Accuracy

To ensure your systems are accurately detecting the right money laundering typologies, your detection models should utilize machine learning to ensure continuous optimization.

Advanced solutions that feature AI and ML technology helps correspondent banks manage the risk of their correspondent customers.

With NICE Actimize solutions, you can:

- **Eliminate basic, static customer segments:** Strengthen your detection and manage risks with advanced, accurate, and dynamic segmentation of respondent banks for accurate activity monitoring and peer comparison.

- **Have dedicated out-of-the-box correspondent detection models, optimized by ML**

- **Configure tuning to meet the risk profiles of correspondent relationships:** Be confident in your alert settings and deploy models faster with full do-it-yourself tuning capabilities. Our robust tuning dashboards come complete with model performance metrics, champion-challenger model simulation capabilities, and tuning impact analysis.

- **Reduce noise and identify suspicious activity:** Unlock superior alert quality with smart model tuning that optimizes model performance with full tuning cycles, while still providing full model governance.

- **Detect anomalies:** Add an extra layer of defence to detect criminals using correspondent networks to launder their illicit wealth with Actimize's advanced anomaly detection.
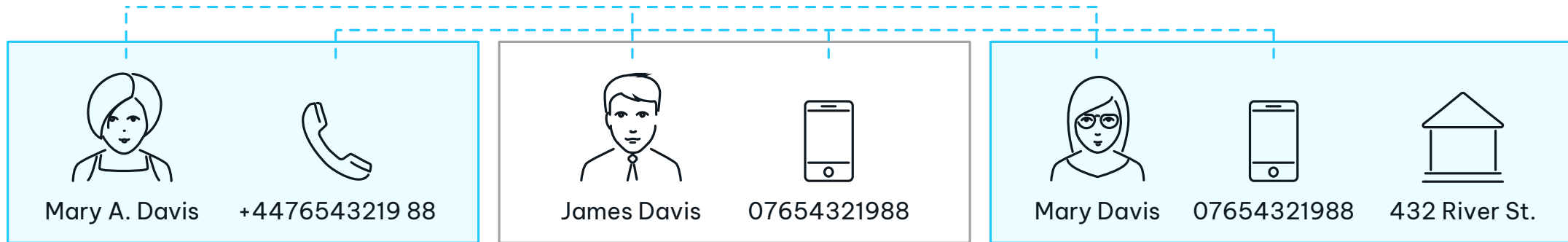
NICE Actimize

Data Enriched Identity Resolution

Given the originators and beneficiaries of correspondent transactions are not direct customers of your organization, it's difficult to understand the legitimacy of transactions between counterparties. Identity resolution resolves duplicate entity records and gives you a consolidated entity profile. It helps with identifying previously disconnected relationships that were present across disconnected profiles. Identity resolution not only resolves duplicate records—it also uncovers hidden relationships, accurately linking related parties for a consolidated view of the parties and associated relationship network.
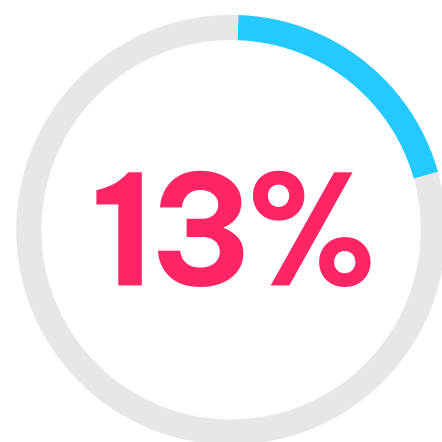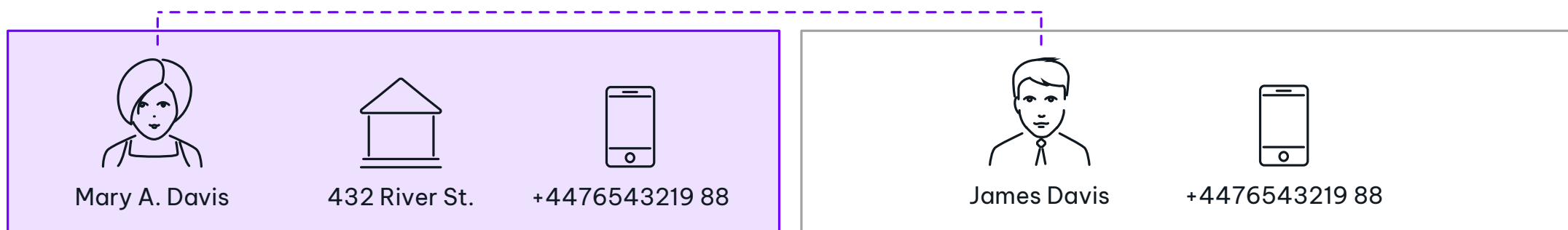
Original Records

Mary A. Davis   +4476543219 88

James Davis   07654321988

Mary Davis   432 River St.   07654321988
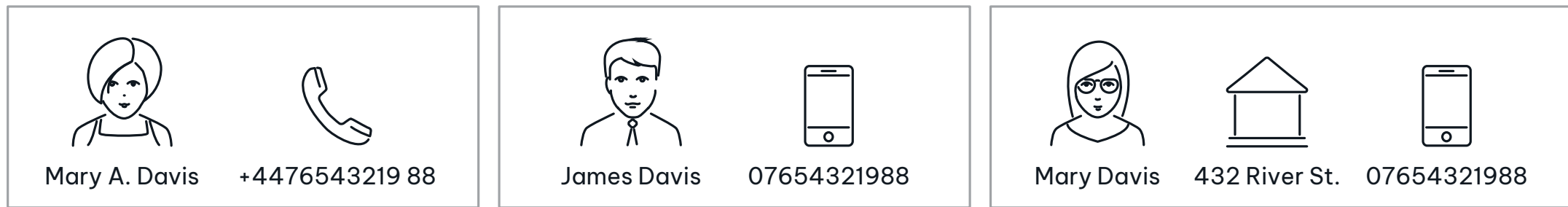
Identified Connections

Mary A. Davis   +4476543219 88

James Davis   07654321988

Mary Davis   07654321988   432 River St.

Resolved Entities and Identified Relationship

Mary A. Davis   432 River St.   +4476543219 88

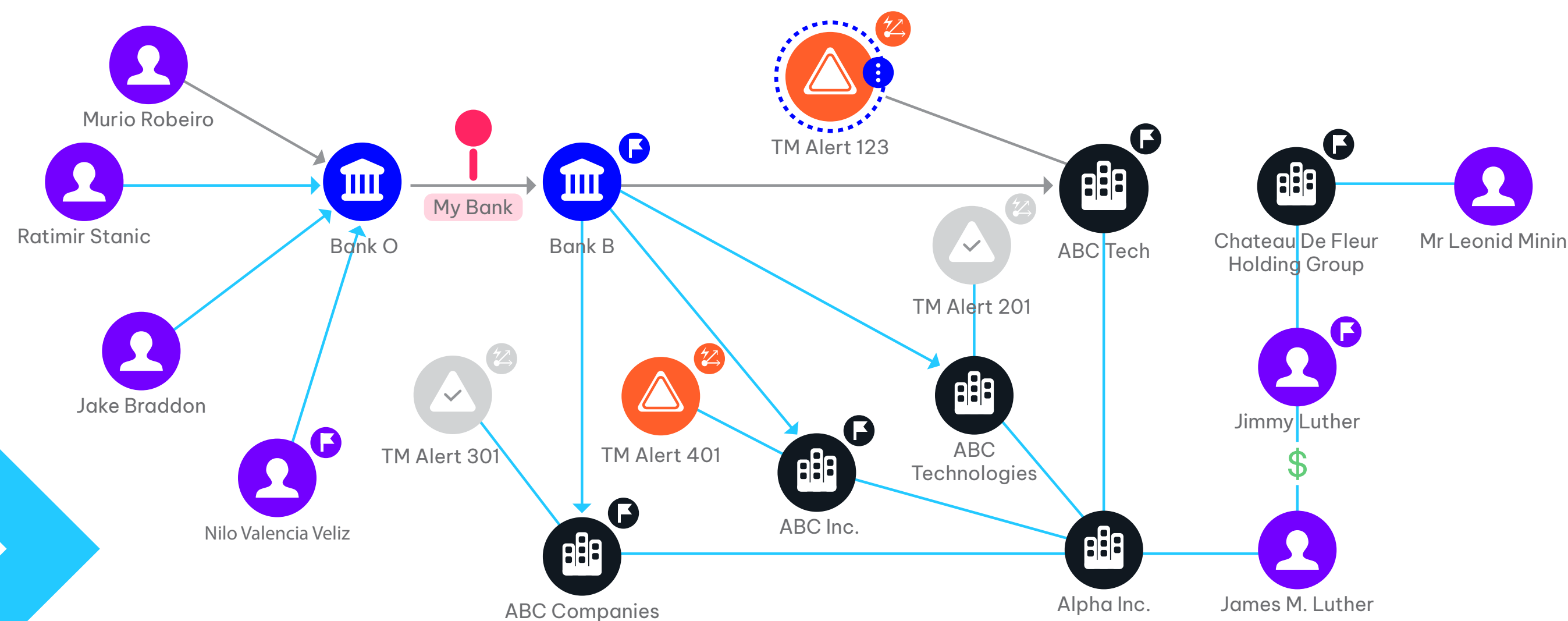James Davis   +4476543219 88

13%

Reduce false positives by

39%

Slash staffing costs due to efficiency gains

NICE Actimize

Understand Network Risk

To understand the legitimacy of transactions between counterparties, network analytics should be employed to discern relationships and connections between those parties. It can also be used to emphasize or bring attention to potentially suspicious connections or activities among these parties. Connect the dots and deliver greater clarity to your correspondent banking relationships and transaction flows with network analytics. You can:

- Enrich known transaction and counterparty information with additional third-party data

- Increase relationship clarity by linking parties through historical information

- Find suspicion by identifying unusual links between seemingly disparate parties

- Provide suspicion clarity to investigators for filing decisions
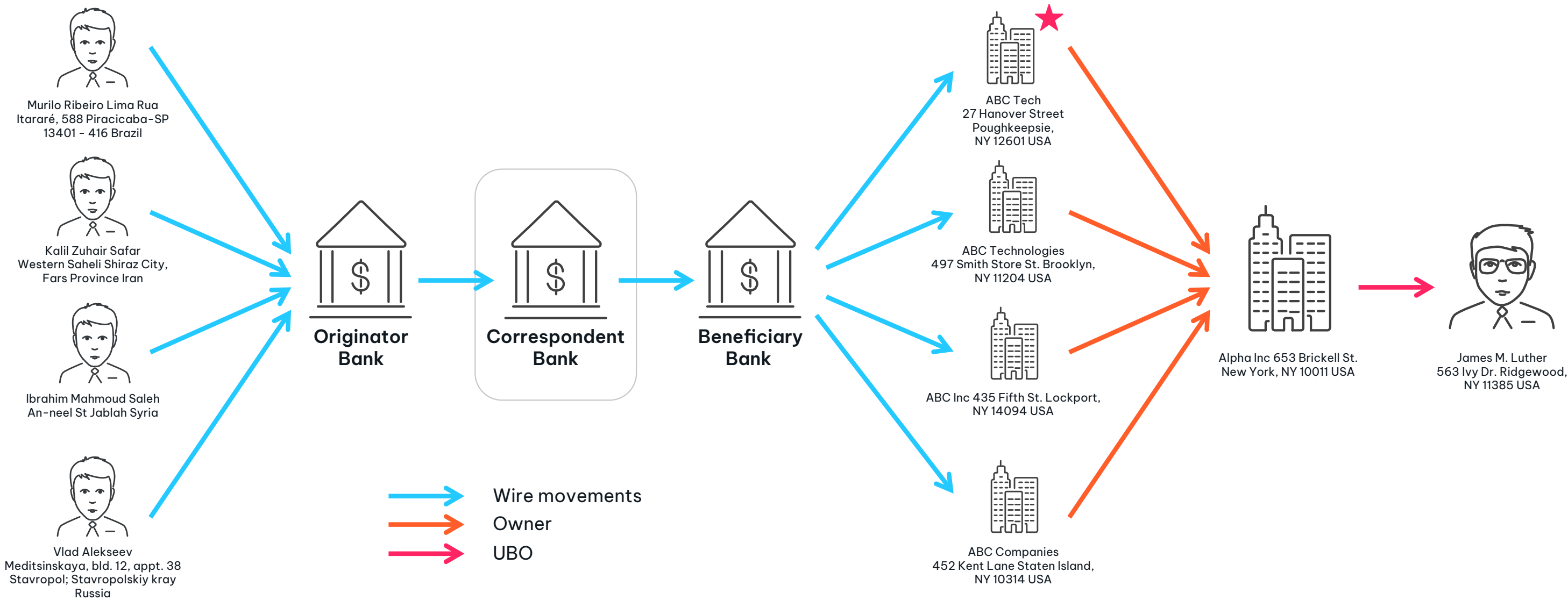
NICE Actimize

Network Analytics Use Case

In this visual, the transaction monitoring solution recognizes that James M. Luther is the ultimate beneficiary of four different payments. These payments appear to originate from mules and are structured through multiple shell companies which are ultimately owned by James M. Luther.

A system that is not using network risk analytics would be unable to identify the suspicious activity. In addition, they would not be able to link the seemingly disparate transactions and parties as being related and the transactions benefitting a single ultimate beneficiary. Using network risk analytics, the system recognizes the suspicious activity and can build relationship connections which would otherwise go unnoticed.

NICE Actimize

Specialized Correspondent Banking Dashboards

Specially designed risk insight dashboards for monitoring correspondent banking transactional activity and connections help teams understand and manage their risk portfolio. These dashboards can visualize suspicious and risky money movements across correspondent banking networks.
In addition, they help to identify excessive movements between respondent banks and identify respondent banks which represent the highest risk to your organization, either because of high alert volumes or significant activity with high-risk jurisdictions. Maintain control of your correspondent banking risk quickly with easy-to-analyze visual dashboards.

NICE Actimize

The Next Step in Understanding Counterparty Risk

The challenges of understanding counterparty risk while still maintaining valuable correspondent relationships are complex and dynamic. Fortunately, the era of de-risking is in the past. By implementing the latest advances in technology, in consolidation with comprehensive strategies, FIs can confidently manage the end-to-end risk associated with respondent banks and their customers.

With NICE Actimize correspondent banking solutions that are powered by advanced technology, FIs are empowered to detect suspicious activities early, making 'de-risking' a relic of the past. Safeguard your correspondent banking relationships, comply with regulations, and achieve greater clarity through advanced technology and analytics with these cutting-edge AML solutions.

Contact us →

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

www.niceactimize.com