NICE
ACTIMIZE

Insights Article

Mitigate AML Risk in Correspondent Banking Without Resorting to De-Risking

Introduction

According to the McKinsey Global Payments Map, cross-border payments through correspondent banking represent 20% of the payments industry's total transaction volumes (domestic and cross-border).

Correspondent/respondent banking relationships truly are vital to the global financial system. They provide access to financial services across jurisdictions to banks and their customers, facilitating international trade, economic growth, global development, and financial inclusion.

However, due to the indirect relationship between the bank facilitating the payment and the originator/end customer, correspondent banking is inherently more susceptible to money laundering than direct originator bank-to-beneficiary bank payments. As a result, financial institutions require significant AML and KYC processes to ensure they are not inadvertently offering services for illicit activity.

Correspondent banks must manage the risks associated with their services while remaining profitable.

Data from BIS shows the number of active correspondent banks worldwide dropped by 3% in 2019 and roughly 22% between 2011 and 2019. While fewer financial institutions offer correspondent banking services, the volume of cross-border payments is continuing to grow. This leads to a higher concentration of transactions and, therefore, a more significant risk for active correspondent banks.

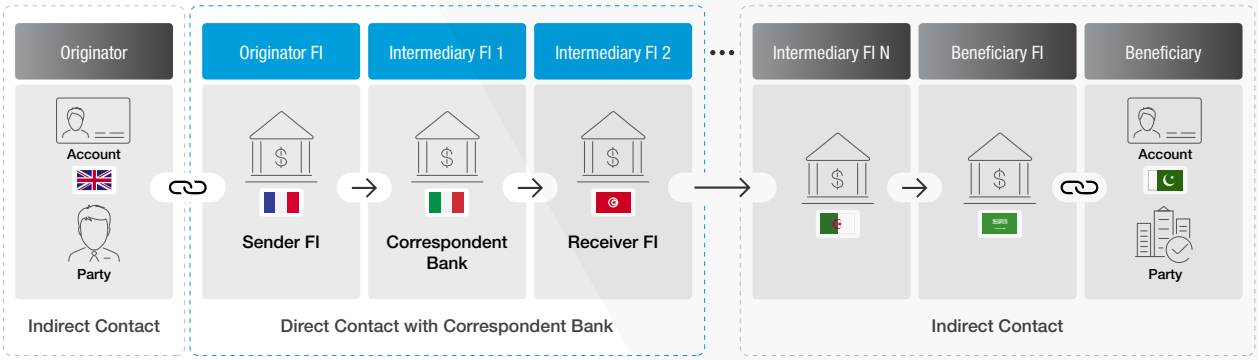
The main factors causing the drop in correspondent banking services are the difficulties in mitigating correspondent banking risks, the increased compliance costs, and reduced profitability that come with effectively mitigating these risks.

Technology solutions now exist that help correspondent banks manage the risk associated with correspondent banking without the need to reduce their customer portfolio through de-risking. Utilizing dedicated technology, financial institutions can get complete risk coverage, helping them better understand their respondent banking relationships and their customers' customers and mitigate any exposure to associated financial crime risk.

The AML Challenges Associated with Correspondent Banking

With the correspondent bank not in direct contact with all the underlying parties involved in a transaction,

they are at a high risk of providing services to bad actors looking to exploit financial systems and launder money from illicit activities.



Often correspondent banks cannot verify the identity of the originating and end customers, establish the source of the funds and wealth, and fully understand the true rationale behind transactions. As a result, without the right controls or technology in place, correspondent banks can unknowingly facilitate money laundering through their Vostro accounts.

> 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.

Without the ability to rely on their own KYC controls, correspondent banks place significant reliance on the respondent bank's controls, checks, and overall compliance framework. Any oversights in assessing the risks present in a respondent banking relationship can lead to significant consequences, including:

- Regulatory fines
- Civil or criminal prosecution
- Restrictions on financial activity
- Reputational damage
- Reduced customer confidence
- Loss of future business
- A drop in share price if publicly listed

With so much at stake, correspondent banks must spend significant time and resources onboarding and monitoring their respondent bank relationships.

During onboarding, many financial institutions utilize the Wolfsberg Correspondent Banking Due Diligence Questionnaire framework to understand the existing AML policies, processes, risk controls, and governance of potential respondent banking relationships. While the Wolfsberg Questionnaire helps guide the discovery of a financial institution's AML practices, it only acts as an aid and should not be solely relied upon. To ensure tolerable risk levels, many relationships require more in-depth information gathering, including on-site visits and discussions with senior leadership and relevant stakeholders.

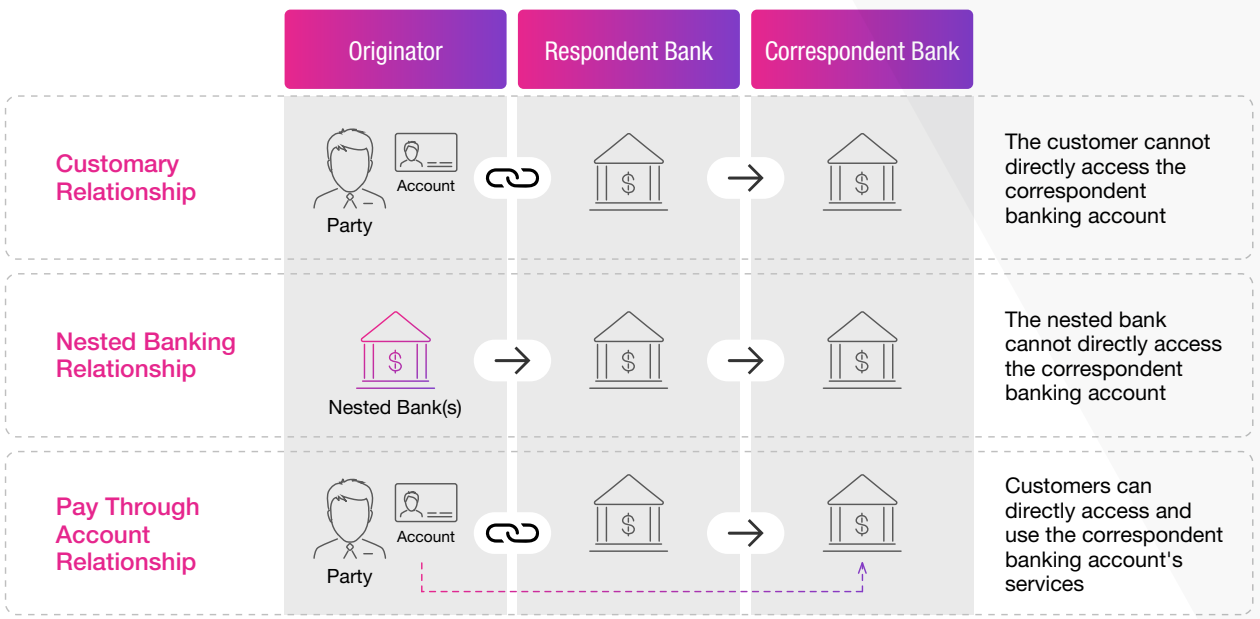
Post-onboarding, robust transaction monitoring is essential. Payment information can allow correspondent banks to ascertain the originator and beneficiary of the funds, the intermediary banks involved, and the intent of the transaction.

Correspondent banks can also implement additional processes to reduce risk further, including performing due diligence and screening on all parties mentioned in payment messages (Know Your Customer's Customer (KYCC)). In addition, financial institutions can raise inquiries with respondent banks seeking additional information on the transaction to allow them to make a final investigation decision.

While these additional measures reduce the risk present in their portfolio, they are often costly and time consuming for correspondent banks. Financial organizations must develop their AML-KYC processes to match internal risk appetite and meet any external compliance requirements while also ensuring the profitability of their services.

High-Risk Counterparties

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



Higher-risk relationships include those involving:

- 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.

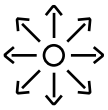
> Both pay through and nested relationships provide third parties (a party other than the correspondent and direct respondent bank) access to the Vostro account. This reduces the financial transparency of transactions and increases the risk of financial organizations unknowingly facilitating money laundering. One in five payments on SWIFT is nested, requiring greater scrutiny on behalf of the correspondent bank to assess the risk present adequately.

With complex financial interactions, potentially involving multiple correspondent/respondent banks, financial organizations can also expose themselves inadvertently to providing services to very 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. US banks are prohibited from establishing, maintaining, administering, or managing accounts for foreign shell banks.

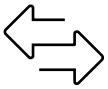
High-Risk Transactions

Several transactional indicators raise cause for suspicion when it comes to correspondent banking activity. These indicators can include:



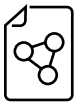
Burst in originator or beneficiary payment activity

Round amount transactions for example, $700.00



Transfers to or from high-risk jurisdictions, institutions, or individuals

Excessive concentration of payments between counter parties or respondent banks



Identification of opaque network relationships between counterparties

Excessive deviation in counterparty transactions with no economic justification

Suspicious payment messages or attempts to strip payment messages

Downsides of De-Risking Correspondent Banking Portfolios

With growing regulatory expectations, the rising cost of due diligence, and lower margins associated with correspondent banking, many financial institutions have begun to de-risk their correspondent banking portfolio. This means scaling back or terminating relationships with high-risk counterparties.

However, de-risking correspondent banking portfolios is not the only answer to addressing counter party risks and has many negative consequences. Banks severing relationships leave a void in financial services often filled by less compliant, less regulated, or entirely unregulated channels. This makes it easier for true money launderers to place, layer, and reintroduce their profits into the financial system. This also forces legitimate transactions into alternative channels that bring additional risk to the originator and beneficiary.

De-risking cross-border payments has considerable effects on the global financial system, destabilizing economies, particularly in developing countries. Cutting off or limiting correspondent banking services to countries creates financial exclusion and has significant social and political implications.

Take, for example, countries across Latin America and the Caribbean whose GDP relies considerably on remittances sent from families working in the United States. De-risking correspondent banking relationships affects cross-border payments to these countries, disrupting residents' free cash, well-being, and spending and, therefore, the country's economy. In addition, de-risking can make it difficult for people to purchase imported goods, pay educational fees for international students attending universities overseas, or even prevent people from seeking medical attention in more developed countries.

De-risking correspondent banking removes risky relationships and reduces the overall risk of facilitating money laundering for financial institutions, but it doesn't solve the problem; it passes the risk onto someone else and has numerous unintended consequences.

Financial institutions shouldn't let criminals dictate how and where they operate. Instead, they should look for smarter, more cost-effective AML strategies that reduce the risks present while also maintaining access to correspondent banking services for all legitimate transactions.

How Technology can Transform Correspondent Banking

The answer to enhancing effectiveness and reducing cost for AML/CFT compliance in correspondent banking is implementing new technology that manages risk without the need to de-risk. Through innovative, tailored software solutions, financial institutions can reduce the cost of AML processes and safely open the door to a more significant number of profitable relationships.

Performing the enhanced due diligence required for a single high-risk counterparty can cost tens of thousands of dollars per year. If the fees recouped from the client do not outweigh the AML spend, it becomes an untenable relationship, losing money for the bank.

[1] LexisNexis. (2020). True Cost of Financial Crime Compliance Study Global Report. LexisNexis Risk Solutions. https://risk.lexisnexis.com/global/en/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report

Correspondent banks must find a suitable trade-off in their AML procedures, protecting themselves and minimizing risk while being profitable. With advanced technology in place, financial institutions can obtain all the available data to take an entity-centric view of activity. This streamlines their compliance procedures and leads to a better understanding of respondent banking partners and the customers they serve.

According to AML experts, analysts spend up to 80% of their time gathering data instead of analyzing data. With smart software in place, correspondent banks can dramatically reduce that figure and get their AML teams working to solve issues instead of finding the required data.

A 2020 global compliance report[1] showed the cost of financial crime compliance is now almost $214 billion, an 18% annual rise. North America saw the most significant jump, 33.3%, to $42 billion.

The report also analyzed mid to large firms in the Netherlands, Italy, France, and Germany that spent 50% or more of their compliance budget on technology. It found these firms had significant reductions in their average annual compliance spend compared to equivalent companies that spent over 50% of their budget on labor. Companies focused on technology also saw reduced negative impacts (17%-25%) for compliance procedures affected by the COVID-19 pandemic - these procedures include risk profiling, increased workloads, onboarding delays, and challenges in KYC data access.

Technology Solutions for Correspondent Banking AML

Software solutions are available to help reduce money laundering exposure while maintaining more relationships with respondent counterparties.

Technology reduces compliance spending to increase profitability while streamlining KYC and screening processes. It allows users to:

- Simplify the capturing of onboarding information in line with the Wolfsberg Questionnaire.
- Screen respondent banks against sanctions lists, PEP lists, adverse media and other potential risks.
- Visualize relationships to quickly understand connections between entities and pinpoint suspicious transactions between counter parties.
- Supplement existing information with third-party data, for example, with a list of existing Nostro accounts for each counterparty from Bankers Almanac.
- Utilize automated triggers for continuous monitoring and risk reassessment (e.g., a sudden increase in transaction volume and a higher concentration of counterparties between respondent banks in high-risk jurisdictions).

With robust transaction monitoring and investigation technology solutions, correspondent banks can:

- Effectively assess payment messages for money laundering red flags
- Build and visualise counterparty relationship networks and associated transaction flows
- Improve detection and alerting for suspicious activity, taking into consideration network risk
- Gain insights into counter party risks with internal and external data enrichment
- Detect hidden nested banking and other high-risk KYCC relationships
- Understand correspondent risks at an enterprise level
- Assess evolving correspondent typologies and implement appropriate monitoring coverage

Summary

Correspondent banking is a vital service in the global financial system. But de-risking, resulting from the high risk of money laundering and the rising compliance costs, threatens to limit or restrict future cross-border payments, pushing criminals into unregulated channels which are harder to track, regulate, and enforce.

Correspondent banking needs an improved, more cost-effective approach to AML. Thankfully, with new innovative software solutions, financial institutions can take an entity-centric approach. They can access more and better data to improve decision-making, enhance monitoring, and detect suspicious activity or behavior more accurately. This reduces risk, increases profits, and prevents the need for de-risking portfolios and the negative consequences it produces.

At NICE Actimize, we offer a range of software to improve correspondent banking KYC and CDD processes and suspicious transaction monitoring. Get in touch today to learn how you can take a more intelligent AML approach that reduces risk while maintaining profitable respondent banking relationships.

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