



CASE STUDY

Enhanced Compliance,
Reduced Costs:
**NetRemit Revolutionises
Cross-Border Payments**



macro global[®]
creating value through innovation



TABLE OF CONTENTS



Introduction	01
Client Background	02
Challenges Faced	03
Solution Implemented	07
Steps involved in Transaction Monitoring Process	12
Results Obtained	17
Conclusion	19

INTRODUCTION

Individuals and businesses of all kinds rely on cross-border transactions to send money to family members overseas, pay suppliers, collect customer payments, and expand into international markets. However, there exists enormous challenges. Laundering of money, fraud, and terrorist funding are posing a huge threat to the global financial system.

Given the immense scale of cross-border transactions and the increasing complexity of financial criminals, it is far more crucial than ever to have effective transaction monitoring. At the same time, businesses expect faster transaction times with lower costs, putting huge demands on remittance service providers to streamline their operations.

Traditional methods of transaction monitoring are frequently slow, laborious, and error-prone, exposing financial firms to both financial losses and regulatory penalties. The demand for real-time visibility, automated screening, and AI-powered insights has never been higher.

One of the UK's remittance service provider encountered this challenge and reached out to Macro Global to revolutionise their cross-border payment operations and, ultimately, protect their business. This case study describes how Macro Global assisted the remittance service provider address these problems by adopting cutting-edge technology and accomplishing real-time compliance, protecting themselves from the ever-changing threat of financial crime.



macro global®
creating value through innovation



CLIENT BACKGROUND

Our client is a well-known remittance service provider in the United Kingdom, facilitating international payments for businesses and individuals from UK to Asian countries. They intended to modernise their existing systems to deliver cost-effective, quick, real-time cross-border transaction services. Notably, the remittance service provider wanted to enhance their transaction monitoring competencies to successfully combat fraud and maintain strong compliance with growing regulatory standards. They wanted to transform their system that could manage large transaction volumes, work in unison with their legacy infrastructure, and take use of cutting-edge technology like artificial intelligence and machine learning. Therefore, the client engaged with Macro Global for their expertise and innovative solutions to offer competitive, secure, and compliant cross-border payments.



CHALLENGES FACED

The UK remittance service provider confronted numerous hurdles in guaranteeing compliance and combating financial crime while processing their cross-border transactions. These challenges have an influence on their operational efficiency, raise expenses, and represent serious threats to their brand and regulatory status.

Challenges Encountered



Here is a closer look at the key challenges the remittance service provider is dealing with:

Inadequate Real-time Screening due to the Massive Volume of Transactions



The remittance service provider processes an enormous volume of cross-border transactions that includes bulk business payments initiated at a time through our back-office platform. This increased the resource requirements for real-time screening significantly as each transaction has to be screened. Implementing effective screening while preserving fair transaction times and client satisfaction is an ongoing balancing act. The remittance service provider required a scalable system that could handle big transaction volumes without sacrificing compliance or causing bottlenecks in their operations. Essentially, they needed speedy and effective real-time screening of transactions.



The False Positive & Negative Issues



When normal transactions are as flagged suspicious (i.e. false positive), it burdens the compliance staff to involve into unnecessary investigations, resulting in operational inefficiencies, higher costs, and dissatisfied customers who face undeserved delays. False negatives, in which legitimately fraudulent activities slip through the loopholes, offer a far bigger risk. They can result in noncompliance with regulations, expose the institution to financial crimes such as money laundering and fraud, and harm their reputations. Minimising both sorts of errors became a significant task.

Legacy System Integration



Like many established remittance service providers, our client relied on legacy systems that were not built to meet the needs of modern cross-border payments and real-time screening technology. Yet, integrating technically advanced transaction monitoring technologies with existing systems is a tedious task. It demands significant investments in technology upgradations, employee training, and process reengineering. This integration procedure could be time-consuming, costly, and disruptive to the remittance service provider's operations.

Evolving Regulatory Requirements



International regulators like the FATF and OFAC and regional regulators routinely publish new regulations and guidance for seamless cross-border payments. Staying on top of these changes and promptly updating the screening techniques is a continuous job. To stay in compliance and avoid penalties, the remittance service provider must be adaptable and sensitive to regulatory changes.

Identifying Behavioural Indicators



Detecting complex financial crime entails more than simply checking names against lists. The remittance service provider needs to look for behavioural signs of suspicious transactions and activity, such as structuring and smurfing. This necessitates a thorough grasp of fraud tendencies as well as the capacity to examine transaction data for minor indicators.

Their monitoring system lacks the necessary parameters and procedures to detect these and other suspicious behaviours. They need to use advanced analytics and AI to improve their ability to spot these more subtle indications of financial crimes.

SOLUTIONS IMPLEMENTED

Recognising the need for a transformational solution, the UK remittance service provider approached Macro Global. Our team of experts devised a meticulous strategy to help remittance service provider to get through the cross-border payment obstacles. Importantly, Macro Global's expertise introduced the remittance service provider to NetRemit, a comprehensive cross-border payments platform equipped with cutting-edge AI and machine learning capabilities.

Building a Fortress: Multilayered Security

Controls

Macro Global assisted the remittance service provider in implementing multi-layered security controls, including advanced measures such as:

Comprehensive Compliance Framework:

The institution was made to implement a tight compliance checklist that included KYC checks for both senders and recipients, regular internal and external audits, extensive staff training on AML legislation, and thorough record-keeping for all transactions.

Implementation of Business and Transaction Rules and Limits:

NetRemit handled the large volume of transactions that were exceeding the institution's existing systems by integrating real-time transaction monitoring within the platform. By utilising, risk-based transaction rules and limits for daily, weekly and monthly transfer thresholds, this system enabled the organisation to examine the profile of every sender, identifying high-risk transactions, high-value transfers,

and multi-intermediary transactions before they were completed. This empowered the remittance service provider to handle transaction volume more effectively while also improving its ability to detect possibly fraudulent activities.

- Furthermore, they improved remittance service provider's Customer Due Diligence processes by establishing significant verification procedures during customer onboarding to screen out fraudulent businesses from the start.
- This included AI-powered systems that could connect attributes and swiftly identify related businesses, even if they tried to conceal or layer their activity.

Analysing Data: Machine Learning for Fraud Detection

The fraud detection capabilities of remittance service provider have been revolutionised by leveraging the power of machine learning within NetRemit. This involved:

Anomaly Detection:

NetRemit's Machine learning algorithms analyse large datasets in real time to detect anomalies and hidden fraud tendencies, offering insights that human analysts would otherwise overlook. This is critical for identifying sophisticated fraud operations.

Customised Rule-Building:

NetRemit empowered the remittance service provider to set up tailored transaction rules and limits to detect suspicious activities such as structuring and smurfing. By combining these customizable guidelines with machine learning insights, the institution ensured its monitoring system remained highly precise and effective in identifying and mitigating financial risks.

API Integration: Gateway for Comprehensive Monitoring

To decrease false positives and get a more diligent picture of transaction risk, our specialists leveraged NetRemit's API integration capability with external databases. This includes:

Core Banking Systems:

Integrating with the core banking systems provides a comprehensive view of consumer activities.

Sanctions Lists and PEP Databases:

Real-time checks of sanctions list (EU, OFAC, HMRC, UNSC) and PEP databases assure compliance and keep out transactions with high-risk people or businesses.

Automated SAR (Suspicious Activity Reports) Generation:

The system automates regulatory reporting, flagging high-risk transactions and assisting compliance teams in submitting Suspicious Activity Reports (SARs) with ease.

This extensive monitoring coverage enables the institution to immediately identify and report suspicious customers and transactions.

Risk Scoring: Balancing Accuracy and Efficiency

NetRemit's AI-powered risk scoring system integrated with marketplace fraud monitoring platforms enables the institution to effectively validate customers and beneficiaries while monitoring transactions for potential fraud and red flags. This includes:

Identity Verification:

Detects theft of identities and document duplication.

CFT Compliance:

Assess customer social behaviour for evaluating terrorist funding concerns.

Global and Country-specific KYC/AML Standards:

The architecture of NetRemit facilitates cross-jurisdictional regulatory compliance, allowing the remittance service provider to carry out transactions effectively. Its automated procedures facilitate expedited onboarding and easy beneficiary identification verification while putting sophisticated eKYC solutions in place to reduce fraud risks and flag suspicious transactions for further scrutiny.

AI-Powered User Behaviour Analysis: Detecting the Unusual

By employing NetRemit's customer and transaction behavioural analysis powered by AI, the remittance service provider identified possible transaction frauds. It analysed user activities to identify unusual transaction patterns such as

- Large, unexpected transfers from unidentified sources
- Unusual transaction amounts that differ greatly from a customer's history
- Unexpected increases in transaction frequency or volume
- Transactions between high-risk countries
- Abnormal transaction patterns, such as frequent transfers between unrelated accounts
- Transactions structured to evade reporting requirements, such as breaking large sums into smaller ones
- Transactions involving politically exposed persons
- Transactions with sanctioned parties/countries

Using transaction data from the past, the system learned to spot irregularities that could be signs of fraud. NetRemit produced high-risk reports that highlighted risk factors and transactions that deviate from the norm while offering insights into consumer behaviour and transaction trends. This all-encompassing perspective aids the institution in allocating resources and prioritising inspections effectively.

STEPS INVOLVED IN TRANSACTION MONITORING PROCESS

1

Understanding the Current Transaction Flow in Their Existing System

- Macro Global experts map the transaction flow identifying entry points, transaction types, and cross-border payment participants such as customers, recipients, and intermediaries inside the remittance service provider's existing system.
- Assessed how the existing legacy systems handle transactions and where they fall behind in terms of real-time monitoring and compliance checks.







2

Customising the Transaction Monitoring Framework in the NetRemit as per Their Business Rules

Macro Global created a new monitoring framework for the remittance service provider with the adoption of NetRemit, the exclusive cross-border payment platform. It entailed:

- Establishing Rules and Parameters:**
Risk-based rules for identifying suspicious transactions are set, including transaction amount thresholds, regional risk indicators, and client profile knowledge. The remittance service provider has the flexibility to update this set transaction rules and limits through the back-office platform, NetRemit Admin Centre.

STEPS INVOLVED IN TRANSACTION MONITORING PROCESS

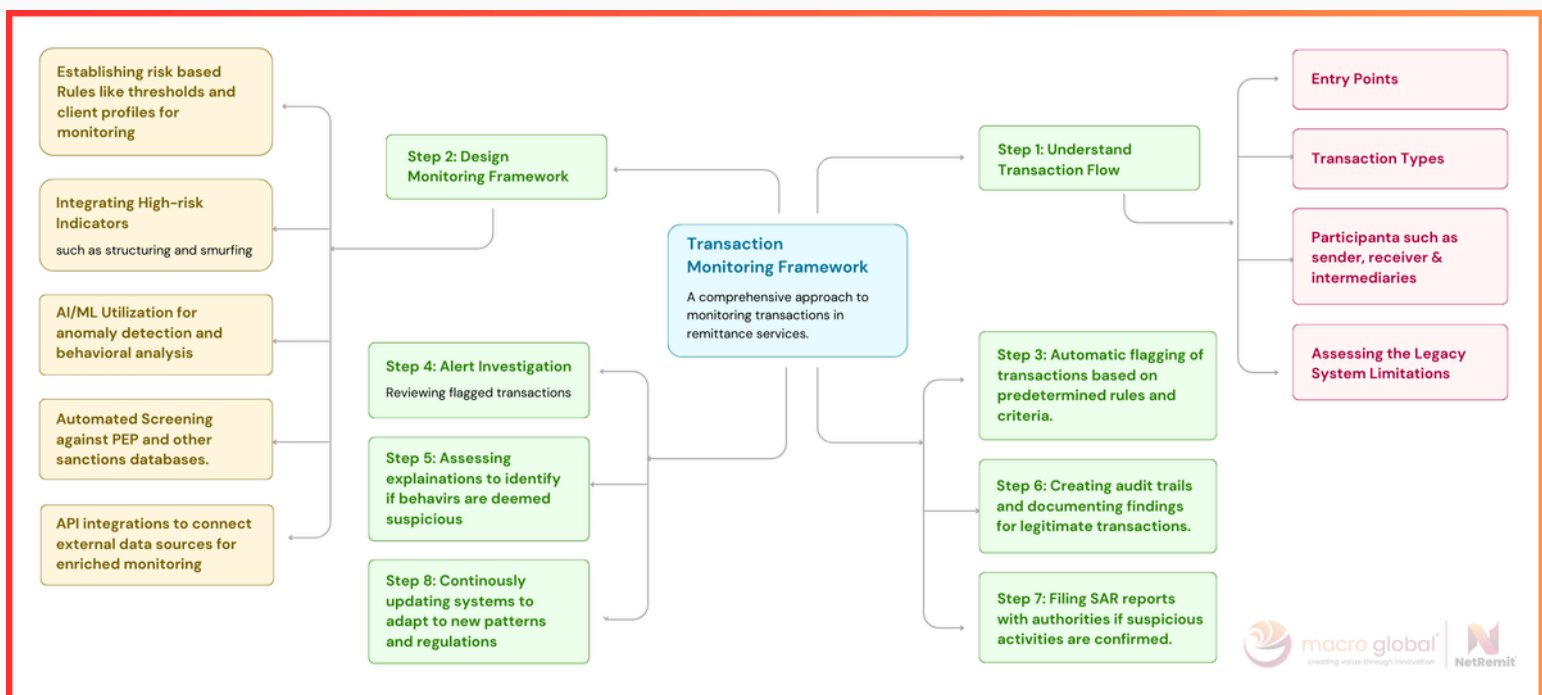
-  **Integration of High-Risk Indicators:**
Identifying behavioural signals specific to potential fraud mechanisms (e.g., structuring, smurfing).
-  **Leveraging Advanced Technologies:**
Use of AI and machine learning algorithms within NetRemit enhanced anomaly detection and improved the system's ability to distinguish between normal and potentially suspicious behaviours based on historical data patterns.
-  **Automated Screening:**
Each transaction underwent automated screening against extensive databases, including PEP lists, sanctions lists, and risk scoring mechanisms before completion.
-  **Risk Profiling:**
Each transaction profile is reviewed against identified high-risk factors, allowing for immediate flags on transactions needing further scrutiny.
-  **Behavioural Analysis:**
The system used historical transaction data to continually learn and adapt, recognizing patterns associated with legitimate transactions versus fraudulent activity. This adaptability minimised false positives and negatives. NetRemit facilitates the client to generate reports on user and transaction behaviour.
-  **API Integrations:**
Integration with external databases enhanced monitoring capabilities, increasing the robustness of risk assessments based on real-time information from regulators and other sources.

STEPS INVOLVED IN TRANSACTION MONITORING PROCESS

3

System-Trigger Alerts

- When a transaction fits one of the specified criteria, the monitoring system sends an automated warning, flagging it for further investigation.
- This moment is essential because it converts raw data into actionable intelligence.



4

Alert Investigation

A transaction investigator carries out:

- Reviewal of the customer's transaction history.
- Contextual analysis of flagged transactions, such as timing, numbers, and involved parties.

STEPS INVOLVED IN TRANSACTION MONITORING PROCESS

- ③ Direct interaction with the customer to ensure that the transactions are legitimate. This includes enquiries about the nature and purpose of the transactions.

5

Documentation and Analysis

- ③ Detail the investigation's findings, including actions and insights.
- ③ If the investigation establishes legitimacy, the case can be closed; however, each inquiry should be kept for audit trails and future study.

6

Determining Suspicious Behaviour

- ③ If the client does not provide a logical explanation for flagged transactions or the inquiry reveals discrepancies or risk factors, the behaviour is considered suspicious.
- ③ It will be raised to higher levels of the institution for appropriate action.

7

Filing Suspicious Activity Report

- ③ If the activity is identified as suspicious, the client is asked to file SAR to regulatory authorities.
- ③ This is an important legal step in AML compliance, since it helps to keep the financial system running properly.

8

Regular Monitoring and Updating of Systems

- Continuously calibrate and improve transaction monitoring techniques, adjusting thresholds, scenarios, and regulations in response to developing patterns, prior investigations, and regulatory changes.
- This is an essential component of the monitoring and control phase of AML procedures.



RESULTS OBTAINED

The adoption of these measures, facilitated by NetRemit and led by Macro Global's expertise, resulted in a dramatic change of the UK remittance service provider's cross-border payment operations. They were capable of:

Compliance Costs Dropped:

Automating KYC/AML checks and other compliance processes resulted in a 25% decrease in manual review hours, freeing up compliance staff to focus on higher-value tasks. This automation, alongside improved data validation, reduced the potential for errors in compliance reporting, leading to a 10% reduction in the estimated risk of regulatory penalties. Overall, these improvements contributed to a 15% reduction in compliance-related operating costs, saving the institution approximately £28,000 per year.

Fraud Detection Soars:

NetRemit enabled the remittance service provider to detect and prevent an average of 15 potentially fraudulent transactions per month, a 30% increase compared to their previous system. This increased vigilance has significantly reduced financial losses and strengthened the institution's brand image.

Faster Transaction Processing Times:

The integration of NetRemit alongside the streamlining of compliance processes, caused a substantial reduction in transaction time. Cross-border payments are now processed in near real time, boosting cash flow and customer satisfaction.

False Positives Reduced:

Fine-tuned their fraud detection procedures, drastically reducing the number of false positives and negatives, allowing the compliance team to focus on genuine disputed activity and minimise unnecessary delays for customers.

Operational Efficiency Skyrocketed:

By automating previously laborious operations, the remittance service provider is able to significantly improve the overall operational efficiency by processing a larger volume of transactions with improved accuracy and speed.

Peace of Mind Secured:

Have a strong, future-proof system in place to handle the intricacies of real-time cross-border payments, allowing the client to concentrate on developing the business and serving their customers with confidence. Reputation of the remittance service provider is preserved.

CONCLUSION

Faced with rising compliance expenses, ineffective fraud detection, and the challenges of real-time cross-border payments, the UK remittance service provider was at a crisis. They tried to strike a balance between speed and security, hampered by outdated technologies and overwhelmed by the sheer number of transactions. The path to compliance felt like navigating a minefield. However, by partnering with Macro Global and deploying the NetRemit platform, the remittance service provider changed its cross-border payment processes. NetRemit emerged as the saviour, offering a multi-layered solution that addressed each difficulty head on.

Macro Global improved compliance processes and unlocked new levels of efficiency and security by utilising AI-powered transaction monitoring, better customer due diligence through machine learning, and easy API integrations. The results speak for themselves: lower compliance costs, higher fraud detection rates, faster transaction times, and a significant increase in customer satisfaction. If your banking institution is facing similar cross-border payment issues, we recommend looking at NetRemit. It's the solution that has enabled us to traverse the complexity of real-time transactions and confidently embrace the future of global banking.



We are here to help you



macro global[®]
creating value through innovation

Please click on the web link below to access our sales desk telephone numbers and email and we will be in touch straight back to you.



<https://www.macroglobal.co.uk/contact-us/>



Macro Global (MG) is the trading name of Macro Infotech Limited, Inca Infotech Ltd & Macro Technology Solutions Pvt Ltd. Macro Infotech Limited & Inca Infotech Limited have Registered Office at 25, Cabot Square, Canary Wharf, London – E14 4QZ and these companies are registered in England & Wales under the registration number 06477763 & 04017901.