The Future of Transaction Monitoring: Better Ways to Detect and Disrupt Financial Crime

SWIFT INSTITUTE

Working Paper by
Matthew R. Redhead
Royal United Services Institute (RUSI)

Global money laundering is estimated annually around USD **800 billion to USD 2 trillion.** Estimates suggest that less than **1%** of the Proceeds of Crime are retrieved by authorities.

Contents

1.0 Glossary 4
2.0 Introduction 5
3.0 Key Findings 7

4.0 The Future of Transaction Monitoring: Better Ways to Detect and Disrupt Financial Crime 9
4.1 Standards, Laws and Regulations 9
4.2 Transaction Monitoring and Reporting In Practice 10
4.3 Transaction Monitoring Strategies 10
4.4 Transaction Monitoring Challenges 10
4.5 Quality Metrics 10
4.6 Costs 11
4.7 So what’s the root cause of the problem? 11
4.8 Innovation 11
4.9 Platform Improvements 13
4.10 Enhancing AML Investigations 13
4.11 Financial Intelligence Sharing Partnerships (FISPs) 14
4.12 FISPs and Transaction Monitoring 14
4.13 Towards system monitoring? 14
4.14 Transaction Monitoring Utilities 15
4.15 Payments Monitoring 16
4.16 Payments Monitoring Prospects 16
4.17 Public Sector-Led Monitoring 16

5.0 Concluding Remarks 17
6.0 Recommendations 19

1.0

Glossary

AML	Anti-money laundering
CDD	Customer Due Diligence
CFT	Counter Terrorist Financing
FATF	Financial Action Task Force
FCC	Financial Crime Compliance
FISP	Financial Intelligence Sharing Partnerships
FIU	Financial Intelligence Unit
JMLIT	Joint Money Laundering Task Force
LEA	Law Enforcement Agency
PET	Privacy Enhancing Technique
RBA	Risk-Based Approach
RPA	Robotic Process Automation
SML	Supervised Machine Learning
STR	Suspicious Transaction Report
TMNL	Transaction Monitoring Netherlands

2.0

Introduction

Transaction monitoring has grown to be a fundamental element in most financial institution’s Financial Crime Compliance (FCC) frameworks.

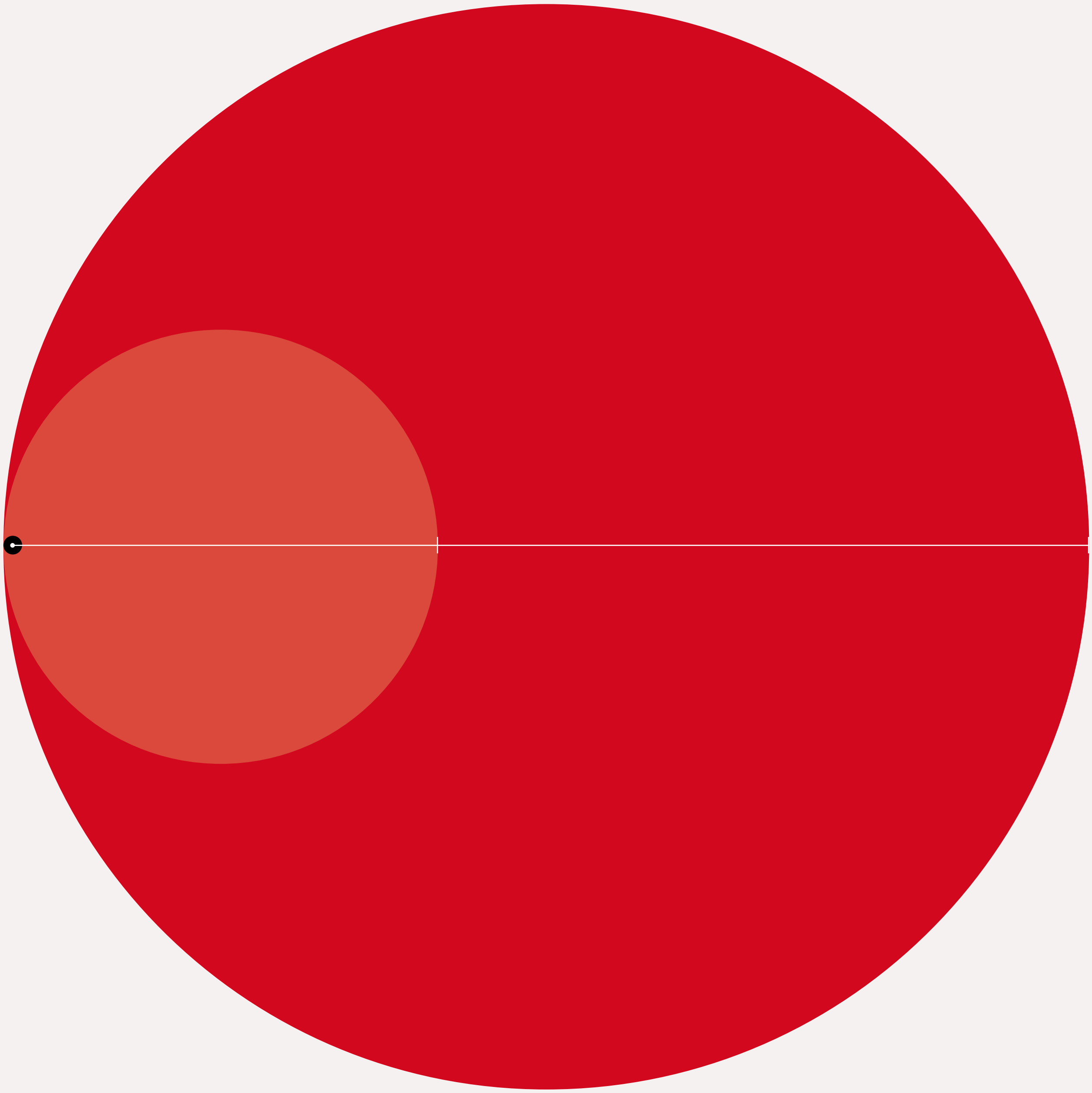
The global anti-money laundering (AML) Regulatory Technology (RegTech) market, of which transaction monitoring is a major part, is growing at an astounding rate. A recent report suggested that its market size of USD 2.2 billion in 2020 was likely to grow to USD 4.5 billion by 2025.

No one knows the exact volume or value of global money laundering, but the most quoted estimates sit somewhere between 2-5% of global Gross Domestic Product (GDP) annually, or around USD 800 billion to USD 2 trillion. Estimates suggest that less than 1% of the Proceeds of Crime are retrieved by authorities.

This research paper analyses the shortcomings of the current transaction monitoring model within the context of the scale of investment, the balance between costs and benefit along with the overall effectiveness of the Suspicious Transaction Reporting (STR) regime. It explores industry initiatives for innovation and reform and provides a set of recommendations to both address existing pain points and to provide potential alternatives and a glance to the future towards the prospect of systemic monitoring.

🟥 $2,000,000,000,000
🟥 $800,000,000,000
■ 1% of $2,000,000,000,000

Global money laundering is estimated annually around **USD 800 billion** to **USD 2 trillion**. Estimates suggest that less than **1%** of the Proceeds of Crime are retrieved by authorities.



3.0

Key Findings

1.

Transaction monitoring and reporting frameworks, as they have evolved over the last three decades, are now in serious difficulties. High volumes of wasted alerts, wasted investigative effort, and little demonstration of value-add to the broader fight against financial crime, combined with escalating costs and regulatory censure – largely disconnected from intelligence outcomes – bring the issue of transaction monitoring reform 'front and centre' for financial institutions and the wider AML ecosystem.

2.

Given this reality, there is a widespread desire across the AML and Counter Terrorist Financing (CFT) ecosystem to reduce waste and improve the delivery of actionable and relevant financial intelligence. Financial institutions are undertaking a range of initiatives to support these goals, including platform optimisation, new tech solutions in the fields of automation and machine learning, risk-focused initiatives and the use of network analysis techniques.

3.

Of the options available within the current AML ecosystem, Financial Intelligence Sharing Partnerships (FISPs) are the best channel through which not only investigators, but transaction monitoring platform specialists, can work together to sharpen platform configuration on matters that might be deemed suspicious, as well as target monitoring on those areas which would add the most value to Law Enforcement Agency (LEA) investigations.

4. Ongoing reforms, institution-by-institution as most are, are only likely to lead to incremental improvements, with uneven impacts across financial institutions. They will not overcome the fundamental disadvantages financial institutions face in seeking to identify criminal behaviour, even with the support of FISPs.

5. Systemic monitoring is likely to be more effective for detecting and possibly intercepting suspicious activity at a network level. A public sector model would likely provide more direct benefits in terms of financial intelligence delivery, while also minimising the legal problems that come with privately managed joint initiatives.

6. Each jurisdiction is likely to have different problems of implementation, suggesting that individual approaches need to be explored. One size will not fit all.

4.0

The Future of Transaction Monitoring: Better Ways to Detect and Disrupt Financial Crime

4.1 Standards, Laws and Regulations

All the ills of AML cannot be laid at the door of transaction monitoring, but in light of the massive discrepancies between effort and result, the value and significance of transaction monitoring, along with the effectiveness of the suspicious transaction reporting regime, there are issues to be addressed.

The global AML rule structure is effectively a 'top-down' cascade, with FATF and its 40 Recommendations at the apex. FATF itself has a remit to set international standards on AML, but as a purely inter-governmental organisation, it does not have legal powers to impose regulations. This falls to FATF's members to take action to make sure that their laws, regulations and institutional frameworks meet the group's minimum standards.

FATF's ongoing role is to evaluate the implementation of the Recommendations at a national level, provide guidance on points of sectoral or financial crime issues, and consider further changes to meet new needs. Throughout their evolution, the 40 Recommendations have retained two core elements: That of **prevention and enforcement:**

- **In Prevention:** Obligated entities are required to carry out three key duties – Customer Due Diligence (CDD) reporting of suspicious transactions to a national Financial Intelligence Unit (FIU), and maintaining records for potential future use by investigators. This is overseen by a regulator.
- **In Enforcement:** FIUs are tasked to process and then disseminate STRs to law enforcement and prosecutorial bodies. The material from the obligated sector is used to support investigations, prosecutions and asset recovery. FIUs also maintain international liaison with regard to cross-border cases.

4.2 Transaction Monitoring and Reporting In Practice

In alignment with FATF's 40 Recommendations and the laws and regulations that accompany them under the Risk Based Approach, some businesses – often small, niche or newer firms – have managed to sustain individual approaches to monitoring. Nonetheless, across the majority of the financial services sector, most financial institutions have adopted a standard model, centred on automated rules-based platforms and high volume alert triage and investigation.

In the first decade of the monitoring requirement, it was common for an automated platform to be built in-house, often using pre-existing models from credit risk and fraud. These days it is more usual to see financial institutions buying in standard models from leading technology vendors.

It is not uncommon for Financial Crime Compliance (FCC) functions to run several different platforms, especially when the financial institution has multiple lines of business and/or operates in many jurisdictions.

This growth in the deployment of automated platforms has had consequences for the scale of technical support necessary to undertake monitoring, often leading to the development of dedicated transaction monitoring teams with FCC technology functions, sometimes supported by vendors or management consultancies.

4.3 Transaction Monitoring Strategies

Of the two main monitoring strategies (rules-based and behavioural), the rules-based approach is the more prevalent, with the choice of rules shaped by a combination of 'industry lore' about how to identify illicit activity and the firm's particular set of risks identified by Enterprise Wide Risk Assessment (EWRA). These rules, often also referred to as 'red flags' or 'typologies', usually come from one of four categories:

- Excessive usage of bank services
- Unusual patterns of funds deposit and withdrawal
- Unusual patterns of funds transfer
- Involvement of high risk factors

A combined sets of rules, thresholds and client segments are often referred to as 'detection scenarios.' A rules-based strategy is not exclusive, however, and in some instances is augmented with behavioural detection methods.

4.4 Transaction Monitoring Challenges

Platform development, day-to-day running, maintenance and periodic replacement require a combination of sustained commitment and resource, and well-managed inputs from a diverse range of stakeholders. However, the basic problems of platform implementation are magnified with transaction monitoring because of the multiple demands that are placed upon it: not only to provide financial intelligence, but also to meet internal cost and regulatory requirements.

Transaction monitoring implementations also typically face a consistent set of practical problems, especially during planning and execution related to:

- Poor data access and quality
- Archaic IT architectures
- Lack of technically skilled staff

Given the complex set of interconnected and ongoing problems related to the development and management of transaction monitoring platforms, combined with the need to balance regulatory compliance and internal costs, there is a is a danger that finding and maintaining that balance becomes the sole focus of a transaction monitoring and reporting framework, rather that the fundamental purpose of identifying valuable financial intelligence.

4.5 Quality Metrics

In other contexts where intelligence is produced, such as national security or law enforcement, the material's effectiveness is typically assessed on criteria such as reliability, accuracy, timeliness, relevance and operational utility. Similar feedback mechanisms are largely missing in AML, however, and financial institutions are largely dependent on self-created metrics to assess their intelligence production performance. The two most commonly cited across the industry are:

a. **The False Positive Rate**: The proportion of alerts deemed neither unusual nor suspicious by AML investigators. This is treated as a rough-and-ready measure of platform accuracy.
b. **The STR Conversion Rate:** The proportion of alerts that lead to an STR. The figure is used to estimate 'True Positives' produced by the platform.

False positive rates vary somewhat between business lines, financial institutions and geographies. However, industry data from a range of sources suggest that the typical proportion of false positives is high, with even the lowest figures suggesting over two thirds of alerts are false positives.

Industry figures on STR conversion rates are rarer, but an EY report indicates very low STR conversion rates for Capital Markets and Wealth transaction monitoring platforms, with 0.2% and 1% respectively, slightly higher for Corporates at 5%, with Retail at 14%.

Amongst those interviewed for this study, the most quoted range for false positives was around 80-90% for conventional transaction monitoring platforms, with STR conversion rates in the region of 2-10%.

In a 2017 survey, Europol, found that only 10% of STRs received by Financial Intelligence Units in the European Union were likely to have immediate investigative value, with the vast majority of reports filed for secondary usage at a later date.

4.6 Costs

In terms of costs, research suggests a current transaction monitoring-linked spend in key markets of over $54 billion. The key driver of cost is personnel, which continues to account for the majority of FCC spending with industry estimated figures ranging from around 60 to nearly 80%.

4.7 So what's the root cause of the problem?

Transaction monitoring, as conducted across most of the industry, is focused on an inherently difficult task: to identify the indicators of suspicious activity, within the limited material of an individual financial institution's transaction data. This is actually a greater challenge than that set out in the foundational document of the FATF 40 Recommendations, which mandates monitoring for consistency of client transactional behaviour and reporting of suspicious instances.

In current practice, a financial institution **needs to understand both what a pattern of suspicious activity looks like**, and how to find it.

In the basic FATF requirement, they need to understand their own customers' behaviours as a benchmark. The latter is clearly more straightforward than the former.

See Recommendation 1 (p19)

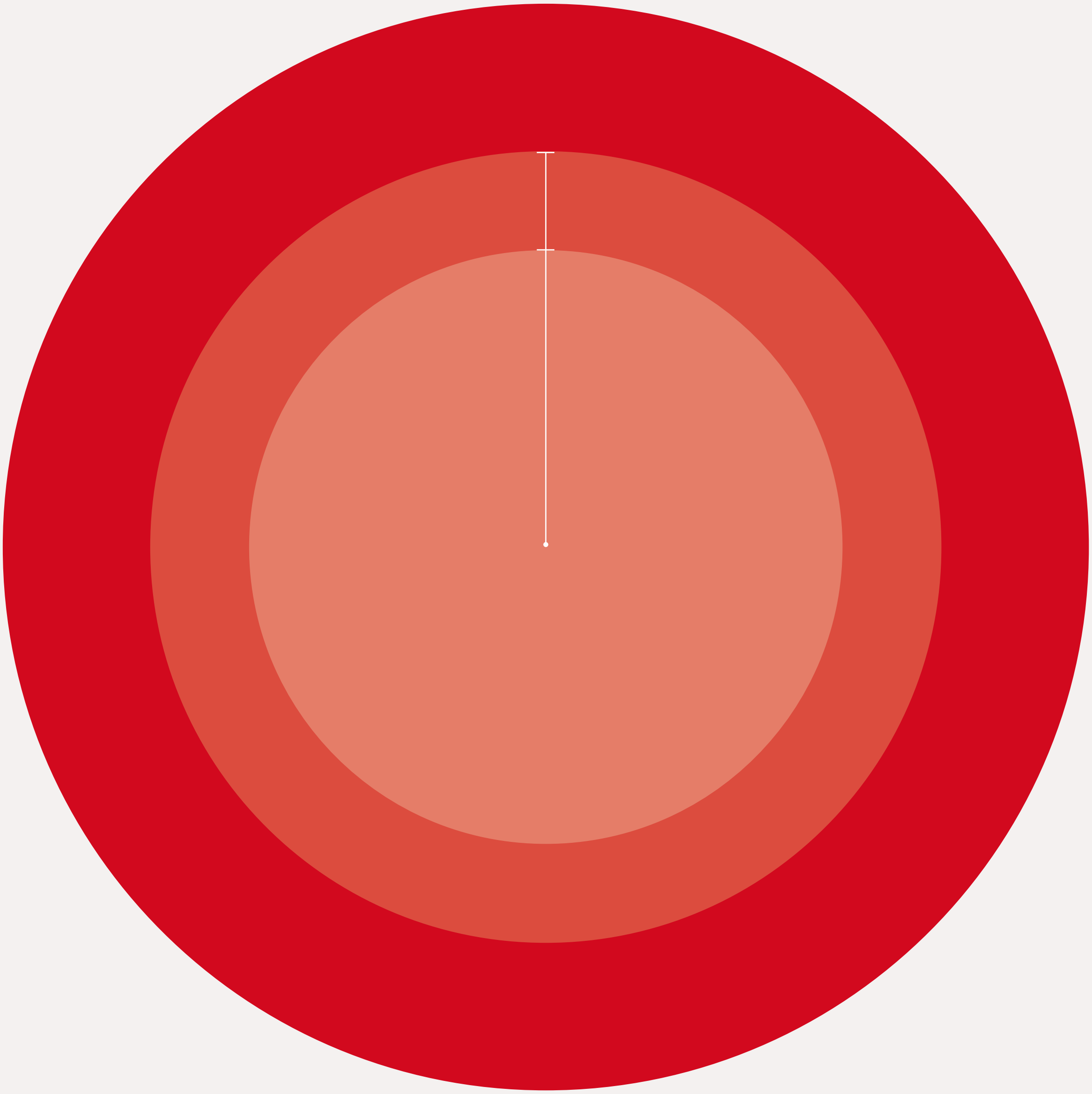
This does not mean that financial institutions should not work collaboratively with partners, private and public, on identifying patterns of suspicion, where feasible. It does, however, suggest that if financial institutions are to have individual institutional AML responsibilities, they should be achievable.

4.8 Innovation

Financial institution initiatives have provided the primary impetus for transaction monitoring reform, at first inspired by a succession of regulatory actions against major institutions, and then, more broadly, by the need to keep up with competitors across the industry. Although many regulators have maintained neutrality towards innovation, several leading bodies

🟥 $54,000,000,000
🟥 80% of $54,000,000,000
🟥 60% of $54,000,000,000

Current transaction monitoring-spend in key markets is over **$54 billion**. The key driver of cost is personnel, which continues to account for the majority of FCC spending with industry estimated figures ranging from around **60 to nearly 80%**.



have openly encouraged it, and FIUs and LEAs have also engaged with financial institutions through Financial Intelligence Sharing Partnerships (FISPs).

4.9 Platform Improvements

Financial institutions have begun to revisit how they use their existing transaction monitoring platforms, and to apply more frequent platform optimisation techniques, such as event-driven or monthly programmes, rather than annual or half yearly reviews, as well as internal feedback loops which allow other FCC functions, especially AML investigators, to feed their current knowledge into platform reconfiguration. A further common initiative is the deployment of new technologies, either to enhance or replace existing platforms, especially amongst top and mid-tier financial institutions.

Of these new technologies, two are now in regular use with transaction monitoring platforms:

- **Robotic Process Automation (RPA)**, which uses software robots (known as 'bots') to undertake simple but repetitive tasks and behaviours at high speed.
- **Machine Learning**, a field of Artificial Intelligence (AI) which uses learning algorithms to categorise data and can be subcategorised into two main areas:
    - **Supervised Machine Learning (SML)**, which is trained on data pre-categorised by humans, where the algorithm learns to sort material into known 'types'; and
    - **Unsupervised Machine Learning**, which identifies patterns across unlabelled data, with the algorithm creating its own categories based on clusters of apparent commonality.

While unsupervised machine learning is yet to be broadly used, RPA and SML have been widely applied to pre-existing rules-based platforms to enhance their performance in several ways, including:

- **Platform Configuration:** SML is being used to segment customers' data into risk categories, both during platform set-up and subsequent optimisation processes.
- **Optimisation:** SML is being applied to testing to assess the productivity of detection scenarios.
- **Alert Handling**: RPA and SML are being used together to prioritise alerts at speed, with SML risk-ranking alerts based on their similarity to past alerts that either led to STRs or were discarded as false positives.

Even with funds, time and good quality staff on their side, innovating financial institutions continue to be hampered by the familiar problem of data. The performance of machine learning analysis is broadly dependent upon access to very large amounts of reliable data, which can prove a problem for financial institutions of all sizes and types. Smaller and younger financial institutions have better quality and more accessible material, but in much smaller amounts, while larger and older institutions have sufficient data, but often of variable quality and format, distributed in many different legacy systems.

In the latter cases, this can necessitate data remediation, standardisation and unification programmes, such as the creation of so-called 'data lakes', bringing together client profile, transaction and commercial data in the Cloud. Attractive solutions though data lakes are in theory, however, they have proved to be long-term 'mega-projects' in their own right, even for extremely well-resourced financial institutions, and prone to major technical barriers and data-sharing issues between jurisdictions with differing data laws.

4.10 Enhancing AML Investigations

Technology has also played a role in efforts to enhance investigator capabilities, through the deployment of increasingly sophisticated Social Network Analysis (SNA) platforms to higher level AML investigators and specialist teams focused on complex products such as trade finance. These new technologies offer financial institutions the chance to exploit better their own data, but do not 'join the dots' of complex criminal networks across multiple financial institutions.

As always there is the issue of cost, if innovation becomes an option only for larger financial institutions who can afford it, then there is a serious risk that financial criminal activity could be displaced into the businesses of smaller financial institutions, who cannot. If innovation is going to have the widest possible impact, mechanisms need to be identified to ensure that knowledge can be shared across the sector.

4.11 Financial Intelligence Sharing Partnerships (FISPs)

Law Enforcement Agencies (LEAs) and Financial Intelligence Units (FIUs) have largely not been involved in internal financial institution innovations or regulatory initiatives, but they have played an important parallel role in the development of Financial Intelligence Sharing Partnerships (FISPs) with financial institutions.

> The first major public-private FISP created was the **UK's Joint Money Laundering Task Force (JMLIT)**, which piloted in 2015, and has since been joined by numerous other initiatives across Europe, North America and Asia-Pacific.

The predominant public-private model is based on regular meetings of senior staff to discuss strategic trends and typologies or to discuss specific cases where suspicious transaction report (STR) filings might be of value to an LEA or disseminate strategic intelligence reports on criminal behaviours and typologies. This and other smaller initiatives are having an enriching effect on the quality of STRs created as a result of public-private interaction, with some positive consequences for levels of criminal disruption. Between February 2015 and June 2020, for example, JMLIT supported 750 cases, with £56 million of illicit assets seized or restrained. The scale of the improvements brought by FISPs remain relatively small however, considered in relation to the scale of financial crime and the volumes of proactive STRs delivered to FIUs.

4.12 FISPs and Transaction Monitoring

The focus of FISPs so far has been on 'downstream' activities of AML investigation and reporting, and less on the 'upstream' matter of what kind of alerts are produced. Partnerships have largely failed to improve the quality and relevance of transaction monitoring alerts and the bulk of proactive STRs that arise from them, which suggests the need for LEAs to use FISPs to provide clearer guidance on strategic reporting priorities, to avoid unproductive reporting.

The value of different detection scenarios might vary over time, or between different types of financial institutions, and FISPs could play a role in guiding these assessments. It would at the very least provide an opportunity to align financial institution and LEA priorities, reduce wastage in the current monitoring and reporting framework, and potentially provide a simpler set of metrics with which financial institutions and regulators could assess whether transaction monitoring frameworks are delivering financial intelligence that can make a difference. Although it would not solve the fundamental fragmentation of the AML ecosystem, it would potentially make it leaner and more focused.

See Recommendations 2 to 4 (p19)

In parallel to these internal financial institution reforms and regulatory efforts, public-private FISPs have proved a useful way to focus financial institutions' AML investigative resources on high priority cases that matter to LEAs, and this study supports their ongoing spread and development. So far, however, they have not been exploited to improve the quality or relevance of the bulk of proactive STRs, and applying the mechanism to identifying suspicious activity on a macro-scale would therefore be an obvious next step.

Of the options available within the bounds of the current AML ecosystem, FISPs are the best channel through which not only investigators, but transaction monitoring platform specialists, can work together to sharpen platform configuration on matters that might be deemed suspicious, as well as target monitoring on those areas which would add the most value to LEA investigations.

See Recommendations 5 to 8 (p19)

4.13 Towards system monitoring?

If monitoring is to create a more accurate understanding of financial crime, the fragmentation of the current approach needs to be addressed at source.

If no institution can presently attain a ‘single point of view’, then the logical step is to create one.

This idea of some version of systemic monitoring has gained some support over the last five years, encouraged by the development of KYC utilities and FISPs. So far, such initiatives have emerged at national levels in only a handful of jurisdictions, most notably ‘Transaction Monitoring Netherlands’ (TMNL), a transaction monitoring utility created in the private sector but with significant official support. Experiments with monitoring across payments architectures or under the auspices of public sector agencies, have also been tried or are being discussed.

4.14 Transaction Monitoring Utilities

In 2018, two separate and unconnected consortia of major banks in the UK (the ‘Tri-Bank Initiative’) and the Netherlands (TMNL) came together to test the feasibility of a national transaction monitoring utility supported by the private sector. Of the two, TMNL has made the most progress, moving from ‘proof of concept’ to a pilot scheme in July 2020, with a scheduled ‘go live’ in June 2021. Led by the jurisdiction’s five largest banks, ING, Rabobank, ABN Amro, Triodos Bank and De Volksbank, TMNL also has broad support from the DNB, the national FIU, and a range of other public sector and industry bodies.

Public details about the early performance of TMNL are limited, but interviews suggest that the project produced encouraging results in early feasibility studies. Rules-based approaches across consolidated data sets reportedly led to reductions in false positive rates and improvements in the detection of previously unknown activity; experimentation with SML, UML and SNA models has led to even better results, with greater precision in the detection of known typologies and the identification of previously undetected flows of funds overseas.

TMNL is still at an early stage, and although reactions around the project are positive, there is little hard data to assess how much better utility-based alerts will prove to be than those created at a financial institution level. Theory suggests that they should be better, but this has yet to be conclusively demonstrated with publicly available information.

Privately-led transaction monitoring utilities also face many of the same challenges of deliverability as their KYC counterparts. Data is the primary issue, and, breadth of coverage is vital. Data quality, consistency and access will also affect performance, and in jurisdictions where transaction monitoring utility participants are struggling with underlying legacy data and systems issues, the process of pooling that data will face the same technical challenges that many international groups already currently face in trying to create a more integrated view of transactions.

The sharing of client data between private institutions falls foul of many jurisdictions’ data laws. It is a definite problem with the EU’s General Data Protection Regulation (GDPR), which does not currently provide specific carve-outs for AML-based sharing, and in some EU jurisdictions is interpreted to prohibit Cloud-based data sharing on which any utility is likely to depend.

The development of shared services by private consortia would also be a potential contravention of many jurisdictions’ competition laws, which typically **stop small groups of market participants acting in concert, and raise questions about the outsourcing of monitoring**, which FATF’s R.17 currently prohibits.

How liability, accountability and regulation will work in practice for an outsourced transaction monitoring utility is not yet wholly apparent.

4.15 Payments Monitoring

There are alternative ways to observe interactions between accounts through inter-institutional payments infrastructures. There are various payments systems within each jurisdiction for different types of payment (whether that be bank-to-bank, credit card payments, etc.), often managed by central banks or shared industry institutions. Information about payments is also shared through transmission mechanisms provided by private organisations such as SWIFT.

Analysing the data from these systems offers a further opportunity to take a systemic view, as several central banks are now finding with SWIFT's Scope tool. Originally deployed at over 30 central banks to conduct real-time macroeconomic monitoring of cross-border flows, the platform has now also been utilised by several of those institutions to analyse SWIFT messages in order to track suspicious activity flows. Payments data has also been used for just such purposes in a recent UK-based project. In December 2018, Vocalink, the infrastructure provider for the UK's Faster Payments System (FPS), launched a 'Mule Insights Tactical Solution' (MITS) with the support of industry body Pay.UK. In October 2019, the Bank of England announced that it too would be developing a pilot project to link its own Clearing House Automated Payment System (CHAPs) to MITS.

4.16 Payments Monitoring Prospects

MITS is reported to have provided fresh insights that did not exist before, including an overview of the structure of money mule networks in the UK retail sector and the existence of a core of hyper-connected mule accounts. If applied in an integrated way across a larger number of payment systems, a MITS-style tool could help financial institutions to identify networks linked to other types of financial crime behaviour, and open the possibility of stopping onward payments for predicate crimes other than just fraud.

In the longer-term, and if applied to regional systems such as SEPA, it could have an international dimension. Alongside operational benefits, a MITS type tool would also sidestep problems with sharing customer data between financial institutions.

Adequacy of coverage would depend on levels of participation from the financial institutions who make up the network, and alerts would still need to be delivered to individual institutions for investigation and reporting. However, payments networks do not have AML reporting and monitoring responsibilities, and it is notable that MITS has developed as a subscriber service.

For the time being, the likeliest prospect of payments monitoring developing more widely would be through government-led initiatives, or a decision by FATF to bring payments networks within the scope of the 40 Recommendations. This would probably prove controversial, however, and does not appear likely to happen in the short to medium term.

4.17 Public Sector-Led Monitoring

A third possible systemic approach is public sector-led monitoring, where the obligation to monitor activity in the financial system is moved to a public sector agency, such as the FIU, an LEA, or under the joint public-private auspices of a FISP.

There are currently no working examples of such an approach, but since 2019, Australia's FISP, the Fintel Alliance, has been working on what it calls the 'Alerting Project', designed to identify suspicious patterns of activity in domestic retail accounts by accessing individual financial institution's transaction databases with Privacy Enhancing Techniques (PET), and then applying machine learning analytics to the encrypted data. Under the current plans, suspect transactions will be delivered to the relevant financial institutions, who will then be expected to provide relevant client details to AUSTRAC, the Australian FIU, for further dissemination and investigation.

Technological implementation would remain a challenge, but many of the problems that hamper transaction monitoring utilities with regard to data sharing, commercial law, liability and regulation would be less likely with direct public sector leadership. From a financial institutions' perspective, the monitoring burden would be reduced, or possibly even eliminated. Nonetheless, a public sector-led model would undoubtedly require significant political will and investment to succeed.

5.0

Concluding Remarks

The theory behind the projects is strong: financial crime is a systemic phenomenon and needs a systemic response. But systemic approaches need to demonstrate that they produce better results than what has come before, and that these can be achieved in a realistic way, given technical and legal constraints. On balance, a public sector-led solution is more likely to deliver intelligence benefits with fewer practical problems.

Altogether simpler from legal and process perspectives, it would also align monitoring directly with investigative priorities. Displacement effects, at least within a jurisdiction, would also be mitigated, because every financial institution would be obligated to provide access to their data. Financial institutions would still need to interact with law enforcement to provide client material on request, but financial institution monitoring responsibilities would be scaled back to confirming consistency of client behaviour and occasional proactive reporting where unusual activity could not be explained by internal investigations.

Nonetheless, other options, such as utilities or payments systems monitoring are not without merit, and might make more sense in certain national contexts, especially if the level of state investment needed to make such a public sector approach possible would be difficult to secure. These are issues which each jurisdiction should explore in their own right, and should be encouraged to do so.

See Recommendations 9 and 10 (p19)

Systemic monitoring still remains more of an idea than a reality, and the projects discussed in the research are immature.

6.0

Recommendations

1. FATF and its member governments to review the language in the 40 Recommendations and national laws to clarify expectations about the focus of monitoring. Ideally, financial institutions should seek to monitor for consistency of client behaviours and report suspicion that arises, rather than seeking to find suspicious activity as a primary activity. Any additional monitoring work should focus on LEA priority areas communicated to FIs through secure means.

2. National regulators, following the US and other examples, should publicly signal support for the prudent use of innovation, including validated new technologies, to deliver AML obligations such as monitoring and reporting, with appropriate protections during regulatory exams and clarity around change risks. The current expectation of ‘parallel running’ of new and old systems for extended periods should be reconsidered as should the stringency of model validation requirements.

3. National regulators, following examples such as Singapore, Hong Kong and the Netherlands, should issue guidance on transaction monitoring model management and governance, providing good practice examples for all relevant activities. Such guidance should be principles-based and allow flexibility for context and a risk-based approach.

4.

National regulators should consider the value of financial institutions annually attesting to the completion of key transaction monitoring platform model management and governance tasks.

5.

FISPs should develop basic feedback mechanisms that identify for financial institutions whether submitted STRs are of immediate use or added to databases as ‘building block’ intelligence. At a next level of sophistication, STRs used in specific investigations should be rated by relevance, timeliness and usability by LEA with timely feedback on individual STRs as well as priority typologies.

6.

FISPs should develop working groups for the discussion of how priority typologies can be translated into transaction monitoring detection scenarios. This should the active involvement of technical specialists from both sectors.

7.

FISP should explore their capacity to act as ‘tasking channels’ for directing the collection of thematically significant intelligence by transaction monitoring in specific investigative areas selected by LEAs, to improve the relevance of proactive STRs.

8.

Alongside examinations of technical compliance and implementation effectiveness, national regulators should include a financial institution’s delivery against FISP defined reporting priorities as an assessment of outcome effectiveness, as suggested by The Wolfsberg Group in December 2019.

9.

FATF should revise the language of its Recommendation 17 with regard to outsourcing of monitoring, providing scope for systemic initiatives where a utility or other systemic solution will provide more coverage than individual FIs.

10.

FATF should monitor the progress of systemic solutions in individual jurisdictions, and develop risk-based guidance to support individual jurisdictional initiatives.

The SWIFT Institute, set up by **SWIFT**, funds **independent research**, supports **knowledge-led debate** and provides a forum where academics and financial practitioners can learn from each other.