SWIFT INSTITUTE

SWIFT INSTITUTE WORKING PAPER

THE FUTURE OF TRANSACTION MONITORING:
BETTER WAYS TO DETECT AND DISRUPT FINANCIAL CRIME

MATTHEW R. REDHEAD

PUBLICATION DATE: MAY 2021

Acknowledgements

The author would like to thank the SWIFT Institute's research sponsorship program for funding this study, with particular thanks to Peter Ware, Nancy Murphy and Louise Agar for their support and remarkable levels of patience throughout the process of research. The author also wishes to thank colleagues from the Centre for Financial Crime and Security Studies (CFCS) at the Royal United Services Institute (RUSI), for their input into the project, with especial thanks to Tom Keatinge, Director of CFCS, Nick Maxwell, Associate Fellow and Director of the Future of Financial Intelligence Sharing (FFIS), programme. Thanks too to Alanna Putze, the CFCS Programme Manager, for ensuring the logistics of project management all ran smoothy. Finally, the author wishes to acknowledge – with considerable gratitude – the contributions from the many interviewees working in compliance, regulation, law enforcement and other sectors, who gave their time to be interviewed by the author.

About The Author

Matthew Redhead is an Associate Fellow at RUSI, a financial crime risk consultant to the Regulatory Technology sector, and a writer on intelligence and national security issues. Prior to his current research and consultancy work, he worked in the Global Financial Crime Risk team at HSBC Holdings for seven years, leaving as Global Head of Strategic Intelligence in April 2018. He has also served as a UK government official at the Ministry of Defence and the Home Office, and has experience in management consultancy and front-office financial services.

Contents

Executive Summary

1. **The Scale of Transaction Monitoring (TM).** The surveillance of client transactions by Financial Institutions (FIs), known as 'Transaction Monitoring' has become a core Financial Crime Compliance (FCC) function. Market research suggests that TM is one of the major growth areas in the global Regulatory Technology (RegTech) market, worth USD 2.2 billion in 2020.[1]

2. **Global Standards and National Laws.** The obligations to monitor client transactions for inconsistent activity and reporting suspicious activity are core elements in the 40 Recommendations of the Financial Action Task Force (FATF), the international standard-setter for Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT). The group's 37 member states have translated these requirements into national laws and regulations.

3. **TM in Practice.** These laws and regulations have led to the evolution of a dominant TM model in the obligated private sector, especially amongst FIs. This model typically comprises automated platforms which apply supposed patterns of illicit behaviour (often referred to as 'typologies' or 'red flags') to transactions, in order to generate alerts. Some models also seek to monitor consistency of client behaviour (often referred to as 'behavioural monitoring.') Alerts are reviewed by AML investigators, who decide whether to discard the alert, refer to an in-house Client Due Diligence (CDD) team, or file a Suspicious Transaction Report (STR)[2] to the national Financial Intelligence Unit (FIU), which disseminates reports amongst Law Enforcement Agencies (LEAs) .

4. **TM Performance.** Data on TM performance is difficult to collate, but what is available provides a dismal picture. TM alert False Positive (FP) rates are between c.70-95%, and alert-to-STR conversion rates between 2-10%. Less than 10% of STRs are reported to be of immediate use to LEAs, and despite being the primary external recipients, FIUs and LEAs provide limited retrospective feedback on STRs' intelligence value. Varied alerting and reporting strategies, poor decision-making and contextual constraints can influence these metrics, but there appears to be a fundamental bias towards the misidentification of innocent activity in the model. This is probably due to an emphasis on trying to find suspicious patterns within a single institution's data, a more complex task than identifying change against the benchmark of known client behaviours.

5. **Costs and Regulatory Frictions.** Despite its uncertain benefits, TM brings significant costs for FIs. FCC teams often find themselves caught between internal pressures to keep costs down, and regulators' requirements that FIs maintain broad coverage of all relevant risks. Attempts by FIs to control expenditure at the cost of coverage have led to significant examples of regulatory censure, further stimulating defensive postures and investment in platforms and staff.

6. **Innovation.** These problems have spurred a widespread desire across the AML/CFT ecosystem to reduce waste and improve the delivery of actionable and relevant financial intelligence. Within FIs, this has led to an increasing tempo of platform optimisation, allied with the use of automation and machine learning to improve testing, the application of pre-existing detection

[1] IReporter, 'Anti-money Laundering Market by Component, Solution, Deployment Mode, End User And Region - Global Forecast to 2025', (September 2020), https://www.reportlinker.com/p05815011/Anti-Money-Laundering-Solution-Market-by-Component-Technology-Type-Deployment-Mode-Organization-Size-And-Region-Global-Forecast-to.html?utm_source=GNW, accessed 1 October 2020.
[2] Referred to by a variety of terms in different jurisdictions, such as 'Suspicious Activity Report' (SAR) in the US and UK.

scenarios, and triaging of alerts. AML investigatory teams have also been increasingly linked into optimisation, refocused on risk over volume management, and equipped with Social Network Analysis (SNA) platforms. Some FIs have also introduced wider risk monitoring directly in the business, or intelligence and analytics functions. Regulators in several leading global financial centres have encouraged many of these reforms and in many jurisdictions, have also worked with FIs, FIUs, LEAs and government departments on Financial Intelligence Sharing Partnerships (FISPs) to improve the scope, quality and ease of intelligence sharing. However, the pace of innovation has been slowed by regualtors' uncertainty about how far to go in embracing new approaches.

7. **Assessing Reform.** The combination of enhanced optimisation regimes, internal feedback loops and new technology have reportedly helped reduce volumes of low value alerts, and new technologies and professionalisation have helped improve investigatory performance. Risk monitoring has also widened the range of financial intelligence to hand for internal risk management. These initiatives should thus be encouraged, and regulators can play important roles in testing new technologies, guiding their appropriate usage, and providing frameworks for applying principles-based guidance to TM management. FISPs could also take a more direct role in helping FIs identify suspicious activities and prioritise risks. Nonetheless, these ongoing reforms, institution-by-institution as most are, are only likely to lead to incremental improvements, with uneven impacts across FIs. They will not, moreover, overcome the fundamental disadvantages FIs face in seeking to identify criminal behaviour, even with FISP support.

8. **Systemic Solutions.** Although there is scope for ongoing behavioural monitoring for CDD purposes within FIs, systemic monitoring is likely to be more effective for detecting and possibly interdicting suspicious activity at a network level. There are different ways to achieve this, including private sector utilities, such as that being developed in the Netherlands, monitoring payments systems, or public sector-led monitoring. Each jurisdiction is likely to have distinctive problems of implementation, suggesting that individual approaches need to be explored. One size is unlikely to fit all. However, a public sector-led model would probably provide more direct benefits in terms of financial intelligence delivery, while also minimising the legal problems that come with privately managed joint initiatives.

Recommendations of this Paper in Brief

R.1 – FATF to clarify language on monitoring for inconsistency and/or suspicion.
R.2 – Regulators to signal public support for technological and other reforms in TM.
R.3 – Regulators to issue regular principles-based guidance on TM management.
R.4 – Regulators to consider methods for application of principles, such as attestation.
R.5 – FIUs/LEAs and/or FISPs to develop metrics and feedback mechanism on STRs.
R.6 – FIUs/LEAs and/or FISPs to develop working groups on TM detection scenarios.
R.7 – FIUs/LEAs and/or FISPs to develop 'tasking channels' for FI intelligence collection.
R.8 – Regulators to integrate operational outcome data [see R.5] into regulatory exams.
R.9 – FATF to revise language of Recommendations to support systemic experiments.
R.10 – FATF to encourage the development of systemic alternatives.

Introduction

A. The Current Context

Transaction Monitoring (TM) has grown to be a fundamental element in most of the financial industry's FCC frameworks. In an interview for this report, a former Money Laundering Reporting Officer (MLRO) from a major international bank remarked that, "for many in the industry, TM has become *the* primary Anti-Money Laundering (AML) control. The money that has been lavished on it is incredible."[3] Indeed, market research suggests that the global AML/CFT (henceforth 'AML') RegTech market, of which TM is a major part, is growing at an astounding rate. One 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.[4]

A sign of success? For RegTech vendors definitely, but in terms of the fight against money laundering and other financial crimes, the answer is less certain. No one knows the 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.[5] To give a sense of scale, this would put the performance of the global criminal economy amongst the top ten of leading national economies. This is a daunting figure, and one made even more so when considered in light of estimates which suggest that less than 1% of the Proceeds of Crime (PoC) are retrieved by authorities.[6] If AML RegTech is a big business, then financial criminality is more lucrative still.

Considering the importance placed on TM, the scale of investment, and the overall results of the regime, it is perhaps worth pondering the balance between costs and benefit. The public furore about the perceived ineffectiveness of global AML efforts, generated by the unauthorised release of US Suspicious Activity Reports (SARs)[7] in September 2020, makes these questions more pressing still. All the ills of AML cannot be laid at the door of TM, but in light of the massive discrepancies between effort and result, the value and significance of TM – along with the effectiveness of the suspicious transaction reporting regime – needs to be addressed. It is perhaps an appropriate time to ask whether there are better ways to proceed.

B. Objectives & Structure

To explore these questions, this paper examines the evolution, current state and potential futures of TM. The paper seeks to:

- Outline the basic regulatory and legal framework of the monitoring requirement
- Examine FIs' current TM practice
- Explore the challenges – internal and external – that have emerged in TM
- Assess and explain the operational performance of current TM
- Review and assess attempts at TM reform
- Look forward to, and assess, alternatives to the current model of TM

[3] Author interview (No.47) with former MLRO based in US, (17 August 2020).
[4] IReporter, 'Anti-money Laundering Market by Component, Solution, Deployment Mode, End User And Region - Global Forecast to 2025', (September 2020), https://www.reportlinker.com/p05815011/Anti-Money-Laundering-Solution-Market-by-Component-Technology-Type-Deployment-Mode-Organization-Size-And-Region-Global-Forecast-to.html?utm_source=GNW, accessed 1 October 2020.
[5] United Nations Office on Drugs and Crime (UNODC), 'Money Laundering and Globalization', https://www.unodc.org/unodc/en/money-laundering/globalization.html, accessed 1 October 2020.
[6] UNODC, 'Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes', *Research Report*, (October 2011), p.11.
[7] The US term for Suspiscious Transactions Reports (STRs).

These objectives are addressed in six corresponding chapters, with a conclusion that provides recommendations on potential next steps for stakeholders in the industry, regulatory, law enforcement and wider AML/CFT policy world.

Chapter 1 provides a brief introduction to the requirements of FATF's 40 Recommendations and the relevant national laws and regulations that have grown from them across member states, while noting variations in language and emphasis in some jurisdictions.

Chapter 2 then takes these regulatory requirements, and assesses how they have been translated into practice by the financial services industry. The chapter reviews the typical approaches seen with respect to TM and its linked functions within an FI's FCC framework, and gives an overview of the platforms, technical teams and AML investigators who facilitate the monitoring and reporting function within FIs.

Commonality of approach does not indicate ease of implementation, however, and Chapter 3 moves into an exploration of the process challenges that come with the development and maintenance of an individual FI's TM framework.

Chapter 4 then shifts to an assessment of outcomes – primarily the effectiveness of TM frameworks to deliver financial intelligence for use within and outside FIs, but also escalating costs and regulatory responses. The chapter also seeks to identify the reasons for TM's apparently poor performance in generating valuable financial intelligence.

In response to the problems outlined in chapters 3 and 4, compliance professionals, regulators and law enforcement officers have expressed increasing unease about TM's effectiveness, and have, over the last decade, developed initiatives to reform it within the bounds of the existing AML framework. Chapter 5 provides an overview of some of the key themes in reform, including:

- **Technology Initiatives**, especially through the use of Machine Learning and SNA;
- **People and Culture Initiatives,** such as professionalisation and closer integration between key TM-linked functions; and
- **Organisational Initiatives**, such as the creation of additional lines of contextual monitoring in the front office, intelligence and analytics functions.

The chapter will also look at the positive roles some regulators are playing in collating and disseminating good practice in TM and nurturing technological innovation, and the support that FIUs, LEAs and relevant government departments have shown to the development of public-private FISPs. The chapter goes on to assess the level of effect that these kinds of reforms have had so far, and whether they have helped to materially improve the operational performance of TM.

Chapter 6 takes this discussion one step further, by then asking whether in some sense the current AML framework – which relies on individual private institutions to act as gatekeepers of the financial system – might not need to be transformed rather than simply reformed, and how that might be achieved through more systemic monitoring options.

Finally, the Conclusion provides recommendations for the way forward, including incremental improvements to the current framework, but also – crucially – medium to long term strategies that could change the character of the AML ecosystem.

C. Methodology

The findings and recommendations contained within this paper are based upon six months of research, which has comprised:

- A literature review of publicly available information from international non-governmental organisations such as FATF, international governmental bodies such as the EU, national governments, regulators, LEAs, legislatures, industry bodies, FIs, major consultancies and AML relevant businesses; and
- 63 semi-structured interviews between March and August 2020, conducted by telephone or internet-based audiovisual platform, with academic, policy, technology, compliance, regulatory, law enforcement and legal experts from jurisdictions in North America, Europe and Asia-Pacific.

As the research developed, initial findings have also been 'road-tested' by informal reviewer feedback and by discussion with a small number of experienced FCC professionals.

D. Scope & Caveats

As is noted above, the FATF requirement to surveil clients' transactions covers all obligated sectors, including banks, Non-Banking Financial Institutions (NBFIs),[8] Designated Non-Financial Businesses and Professions (DNFBPs)[9] and now Virtual Assets Service Providers (VASPs).[10] However, it has impacted most significantly on those entities with the largest transaction volumes – chiefly the banks but also NBFIs such as Money Service Bureaus (MSBs) and other payments related services. Although much of what this report says is relevant to all sectors, its primary focus is financial services, as a shorthand, the paper refers to FIs as the main subjects of interest throughout.

The paper also focuses explicitly on Transaction Monitoring of clients and its linked processes, and excludes other FCC surveillance measures such as Transactions Screening for sanctioned individuals and entities, Politically Exposed Persons (PEPs), and other watchlist exposures, or internal surveillance of staff activities.

[8] Financial institutions that do not have a full banking license and cannot accept deposits from the public, such as insurance providers, credit firms, etc.

[9] Businesses that provide professional services to support financial activities, such as lawyers, accountants, etc.

[10] Businesses that conduct one or more of the following actions on behalf of its clients: exchange between virtual assets and fiat currencies. exchange between one or more forms of virtual assets. transfer of virtual assets.

1 – Standards, Laws & Regulations

The global AML rule structure, of which the monitoring and reporting requirements are a part, 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. It thus falls to FATF's members – and those who aspire to membership – to take action to make sure that their laws, regulations and institutional frameworks meet the group's minimum standards. This in theory means that there can be some variations between different jurisdictions' approaches to meeting FATF's requirements, but in reality, most have tended to exhibit broad conformity with the minimum standards as set out in the Recommendations.

1.1 FATF

FATF was created by the Group of Seven (G-7), the world's leading developed economies, at their summit in July 1989.[11] The group is an inter-governmental body, meeting in plenary three times a year, with support from a small secretariat in Paris. There were sixteen original members, which has now grown to 37 member states, and 2 regional organisations – the EU and the Gulf Cooperation Council (GCC). Over the last three decades, a wider network of 9 'FATF-style' Regional Bodies (FSRBs)[12] has also developed, which, collectively, have a membership of over 200 countries.[13] FATF's ongoing role is to evaluate the implementation of the Recommendations at a national level, provide specific guidance on points on sectoral or financial crime issues, and consider further changes to meet new needs.

1.2 The 40 Recommendations

The first set of the 40 Recommendations were issued in April 1990, and were revised to varying degrees in 1996, 2001, 2003, 2004, with the most recent wholesale revision in February 2012.[14] These changes have brought a wider range of obligated sectors, predicate money laundering offences, and other financial crime types, such as CFT, into the scope of the standards. But throughout their evolution, however, the 40 Recommendations have retained two core elements which can be described as *prevention* and *enforcement*:

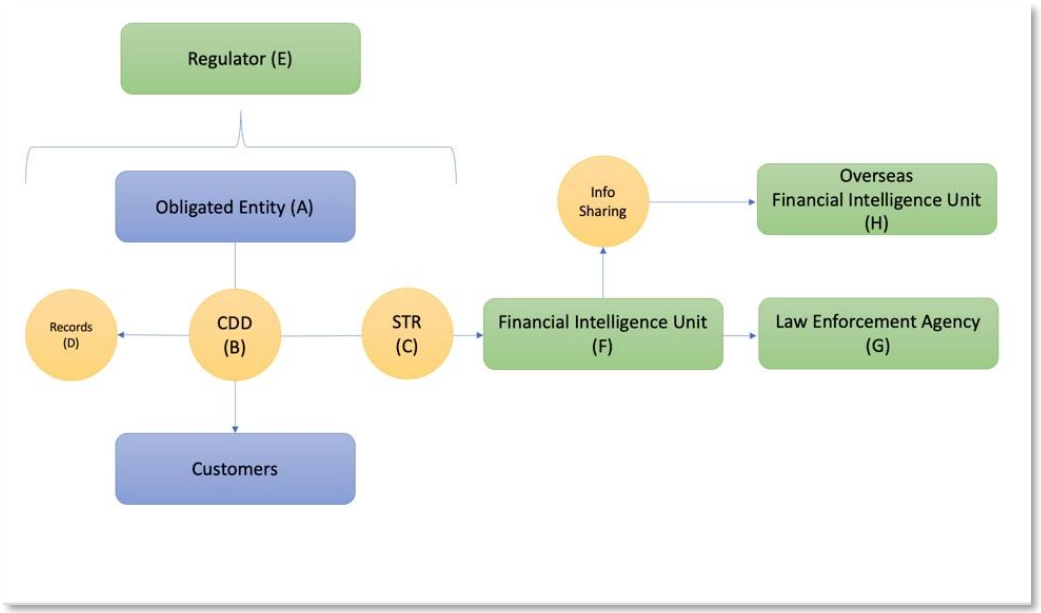
- **In Prevention:** Obligated entities (marked box 'A' in Figure 1 below) are required to carry out three key duties – CDD ('B'), reporting of suspicious transactions ('C') to a national FIU, and maintaining records ('D') for potential future use by investigators. This is overseen by a national regulator ('E').
- **In Enforcement:** FIUs ('F') are tasked to process and then disseminate STRs to law enforcement and prosecutorial bodies ('G'). 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 where Mutual Legal Assistance Treaties (MLAT) exist ('H').

The two pillars are of course linked, because the preventative measures are intended to enhance enforcement. Through CDD, obligated entities can prevent the misuse of the financial system for

[11] The G7 in 1989 were: France, Federal Republic of Germany, United Kingdom, Italy, Japan, United States and Canada.
[12] FSRBs must comply with, and evaluate against, FATF standards to be considered as such.
[13] FATF, 'Countries', https://www.fatf-gafi.org/countries/, accessed 1 October 2020.
[14] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations', (February 2012 – last amendment July 2019).

criminal ends, and through reporting and record-keeping, detect potential crime and support official investigations.[15]

FIGURE 1 – Basic National AML/CFT Structure[16]



1.3 Monitoring and Reporting in Detail

In the most recent Recommendations, the monitoring requirement is expressed as the fourth element within Recommendation 10 (R.10) on CDD. The Recommendation suggests that obligated entries should conduct:

> "Ongoing due diligence on the business relationship and *scrutiny of transactions* undertaken throughout the course of that relationship to ensure that the transactions being conducted are *consistent with the institution's knowledge* of the customer, their business and risk profile, including, where necessary, the source of funds."[17] [Author's italics].

This highlights that the fundamental requirement for FATF is to monitor client transactions for the purposes of identifying inconsistent client behaviour, based on obligated entities' knowledge of the client. It is not to monitor for the purpose of finding suspicious or unusual activity as a goal *per se*. It is initially an ongoing CDD rather than an investigative requirement.

As with other aspects of CDD, R.10 notes that the intensity of this transactional scrutiny should be calibrated by a 'Risk-Based Approach' (RBA), based on the variable financial crime risks that come with differing client profiles, product types and geographies of operation. In higher risk situations, clients should be subjected to more intensive monitoring as one measure of Enhanced Due Diligence (EDD), and vice versa for lower risk situations. Although several aspects of CDD can be outsourced, R.17 states that "scrutiny of transactions" should remain in-house.[18] The

[15] Reuter, Peter, and Edwin M. Truman, *Chasing Dirty Money: the Fight Against Money Laundering*, (Washington, D.C.: International Institute of Economics, 2004), pp.46-48.
[16] Author's simplified version of the diagram found at the European Commission website page, 'Preventing Money laundering and Terrorist Financing across the EU. How does it work in practice?' https://ec.europa.eu/info/sites/info/files/diagram_aml_2018.07_ok.pdf, accessed 1 September 2020.
[17] FATF, 'The FATF Recommendations', (February 2012), p.12.
[18] Idem., p.16.

requirement to report – but notably not to stop – suspicious transactional activity appears later in the Recommendations, in R.20:

> "If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU)."[19]

The Recommendations' Interpretative Notes go on to suggest that suspicious activity might comprise complex, unusual or unusually large transactions that serve no obvious economic purpose.[20]

1.4 Assessing the Recommendations

The Recommendations' approach to monitoring and reporting is a relatively basic framework, with:

- a focus on transactions as a definitive source of intelligence
- inconsistency and suspicion as key criteria for assessment
- external reporting as a primary tool of retrospective action

More detailed examinations of its practical mechanics have been further explored in sector-specific documentation, where FATF has sought to clarify possible ways of approaching some implementation issues in a 'risk based' way. In its 'Banking Sector Guide on a Risk Based Approach,' for example, the group provides further advice on how to assess the consistency of client behaviour, including not only comparing the client with expectations of its own behaviour, but also with peer groups of similar types of customer.[21] The Guide also provides some suggestions around what kinds of monitoring solutions might be appropriate for different types of banking activity; "where large volumes of transactions occur on a regular basis," it suggests, "automated systems may be the only realistic method of monitoring transactions."[22]

But such advice, while valuable, is far from systematic and does not address fundamental ambiguities in the Recommendations' language – especially the definition of 'suspicion' – a concept wide open to both broad and narrow interpretations. Slight misalignments of language in different parts of the Recommendations can also cause difficulties. R.10 highlights monitoring for consistency, and R.20 emphasises reporting on suspicion, raising further questions over whether obligated entities should be monitoring for *both* consistency and suspicion, or just the former, and reporting suspicion by exception. Such variations of language can, of course, make significant differences to operational practice and resource requirements.

1.5 Laws & Regulations

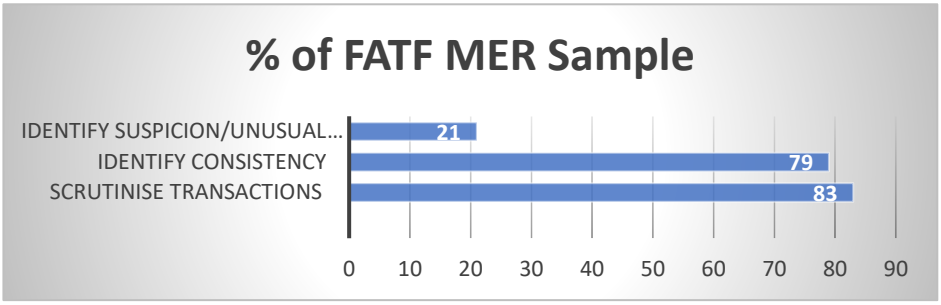
The Recommendations have proved to be a powerful force for shaping national AML policies around monitoring and reporting, and a review of 24 FATF and FSRB jurisdiction-level Mutual Evaluation Reports (MERs) from the 4th Round of Evaluation indicate relatively high levels of consistency across the various jurisdictions.[23] As shown in Figure 2 below, around 80% of those

[19] Idem., p.17.
[20] Idem., p.64.
[21] FATF, 'Guidance for a Risk-Based Approach: The Banking Sector', (October 2014), p.21.
[22] Ibid.
[23] In order to save space, the MERs are referenced to in short form in this footnote with the exception of the first report. Full document details are available in the Bibliography. FATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report', (April 2015), p. 90, p.166; Austria (September 2016), p.134, p.148; Belgium, (April 2015), p.172, p.185; Canada,

sampled stipulate that transactions must be scrutinised for consistency with known CDD records, as per the requirement of R.10, while just over 20% also require obligated entities to monitor for specific additional issues, whether that be suspicious or unusual activity, or indications of money laundering and terrorist finance.

Figure 2 – Type of Monitoring Activity Required in Laws and Regulations

(Sample size 24 Jurisdictions, categories not mutually exclusive)

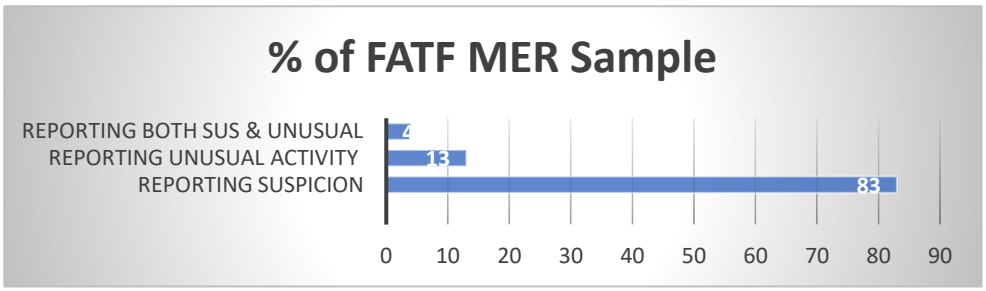


Most jurisdictions do not specify how the obligation should be undertaken, following the RBA recommended by FATF. There are a handful of exceptions, however, such as Mexico and Norway, who have mandated automated platforms for monitoring for FIs, and some other jurisdictions not covered in the sample, such as the Netherlands, have recently encouraged the use of automation where FIs have significant transactions volumes.[24]

There is also considerable consistency around the laws and regulations regarding reporting, as shown in Figure 3. Over 80% of the jurisdictions sampled specify that entities should report on grounds of suspicion, with nearly all of the remainder using the lower standard of 'unusual' behaviour. In one jurisdiction – Mexico – there is scope to report both suspicious and unusual activity.

Figure 3 – Reporting Thresholds for Alerts in Monitoring Laws and Regulations

(Sample size 24 Jurisdictions, categories mutually exclusive)



Timescales for reporting are more varied, however, as shown in Figure 4. Usually working from the baseline of identifying suspicion or unusual behaviour, a quarter of those jurisdictions

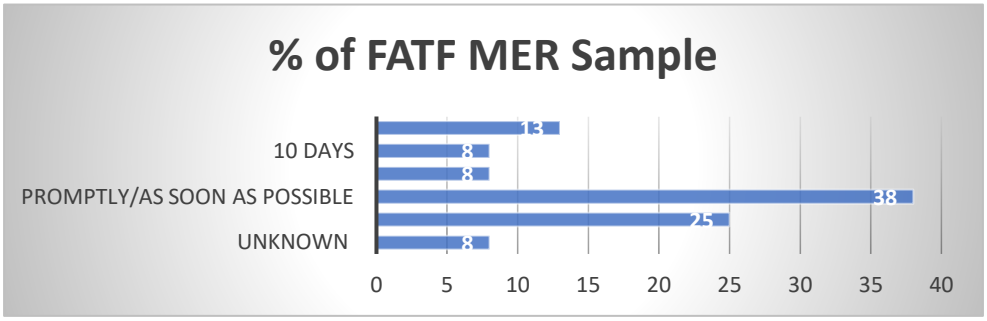
(September 2016), p.141, p.157; People's Republic of China, (April 2019), p.203, pp.220-221; Denmark (August 2017), p.168, p.183; Finland (April 2019), p.176, p.186; Greece (September 2019), p.175, p.188; Hong Kong, China (September 2019), p.188, pp.204-205; Iceland (April 2018), p.139, p.154; Israel (December 2018), p.206, pp.220-21; Italy (February 2016), p.152, pp.168-169; Kingdom of Saudi Arabia (September 2018), p.185, pp.196-197; Mexico (January 2018), p.96, pp.179-181; Norway (December 2014), p.159, pp.170-171; Portugal (December 2017), p.145, pp.158-159; Republic of Korea, (April 2020), p.179, p.189; Russian Federation (December 2019), p.26, pp.283-284; Sweden (April 2017), p.161, pp.171-172; Switzerland (December 2016), p.179, pp.194-195; Turkey (December 2019), p.184, pp.200-201; United Arab Emirates (April 2020), p.231, pp.242-243; United Kingdom (December 2018), p.194, p.207; United States of America (December 2016), pp.200-201, pp.218-219.

[24] De Nederlandsche Bank (DNB), 'Post-event Transaction Monitoring Process for Banks: Guidance', (August 2017), p.7; FATF, 'Mexico Mutual Evaluation Report', (January 2018), p.96; FATF, 'Norway Mutual Evaluation Report', (December 2014), p.159.

surveyed required an immediate report, while 38%, the largest minority of the sample, required reports be delivered 'promptly', 'without delay' or 'as soon as possible.' Around a third of the sample set specific deadlines for reporting, but these covered a wide range from three days in the case of Australia and Russia, to 30 days in the US, Canada and Mexico, unless there are threat to life aspects as in terrorist-linked cases.[25]

Figure 4 – Reporting Timelines for STRs in Monitoring Laws and Regulations

(Sample size 24 Jurisdictions, categories mutually exclusive)



1.6 Conclusion

In summary, the character of monitoring and reporting requirements across the membership of FATF is mostly consistent, and broadly in line with FATF's Recommendations. Most jurisdictions require that obligated entities monitor for CDD purposes and report concerns that arise from that monitoring. Nonetheless, there are some interesting variations and points of diversity within the data. It is noticeable that just over a fifth of the sample have augmented the basic requirement of R.10 to monitor for, as well as report, suspicious or unusual patterns of behaviour. It is also striking that although over 50% of the sample require transactions reporting immediately or soon after a judgement is made, a significant minority of jurisdictions have provided additional time for reporting to take place. Although it is not possible to draw hard conclusions from these figures, this might suggest that in some jurisdictions, there is a perception that creating a valuable STR is a more challenging task than an immediate reporting deadline will allow.

[25] FATF 'Australia Mutual Evaluation Report', (April 2015), p. 90, p.166; 'Canada Mutual Evaluation Report', (September 2016), p.141, p.157; 'Mexico Mutual Evaluation Report', (January 2018), p.96, pp.179-181; 'Russian Federation Mutual Evaluation Report', (December 2019), p.26, pp.283-284; 'United States of America Mutual Evaluation Report' (December 2016), pp.200-201, pp.218-219.

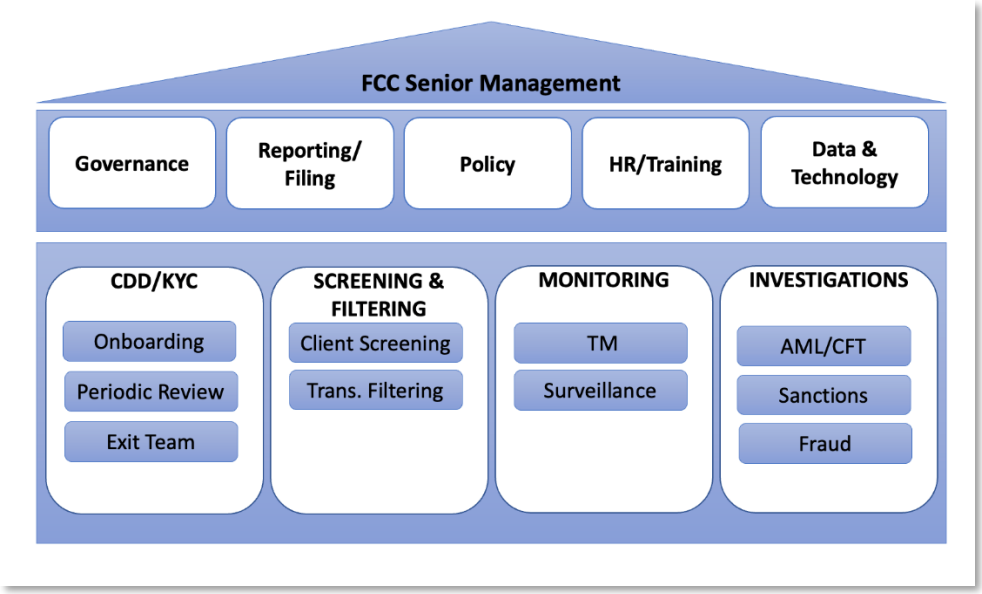
2. TM and Reporting in Practice

FATF's 40 Recommendations and the laws and regulations aligned with them allow some freedom of action to FIs and other obligated entities in how they execute their roles, shaped by a range of factors that help determine their overall risk profile. Under the RBA, it is perfectly feasible for FIs to take distinctive paths, and some businesses – often small, niche or newer firms – have managed to sustain individual approaches to monitoring. Nonetheless, across the wider swathes of the financial services sector, most FIs have coalesced around a dominant, standard model, centred on automated rules-based platforms and high volume alert triage and investigation.

2.1 Structures

Monitoring and reporting functions sit within the FCC structures of an FI. In lower tier firms, those functions can be undertaken by the MLRO, supported by a small team, but from mid-tier FIs upwards, it is typical to see extensive FCC structures, similar to those in Figure 5. Here, multiple cross-cutting functionings sit above core AML controls such as CDD and 'Know Your Customer' (KYC), screening and monitoring.

Figure 5 – Common FCC Structure[26]



FCC structures primarily sit in what is known as the 'Second Line of Defence', creating policies, procedures and controls for the 'First Line' in the business to implement, and the 'Third Line' – internal audit – to review. Although monitoring and reporting are rooted deeply in most FCC structures, as shown in Figure 5, they do themselves share some affinity with 'First Line' activities because of their operational focus on detecting and mitigating risk.[27] As a consequence, TM activities in a FI are sometimes split with the initial assessment of alerts carried out by the First Line, and the conclusion of a STR and the subsequent filing always within the Second in the FCC function.

[26] Author's design based on simplified version of model of framework presented by professional services provider Oliver Wyman. Liu, Yanan, Jayant Ramen (Oliver Wyman), 'Financial Crime Compliance: Current Global State of Play', *Brink*, (15 October 2017), https://www.brinknews.com/financial-crime-compliance-current-global-state-of-play/, accessed 1 October 2020.

[27] Author Interview (No.1) with senior compliance professional based in UK, (2 June 2020);
Davies, Howard, and Maria Zhivitskaya, 'Three Lines of Defence: A Robust Organising Framework, or Just Lines in the Sand?' *Global Policy,* Volume 9, Supplement 1, (June 2018), pp.34-42.

Elements in the FCC framework link together in specific ways to deliver monitoring and reporting; there are close links between Data & Technology functions, TM, AML/CFT investigators and also CDD teams. From a step-by-step perspective, this set of connections looks similar to Figure 6, with:

(1) the receipt of transactions data from core business payments systems

(2) the review of those transactions by the assigned monitoring mechanism

(3) the production of alerts or cases that require dedicated review

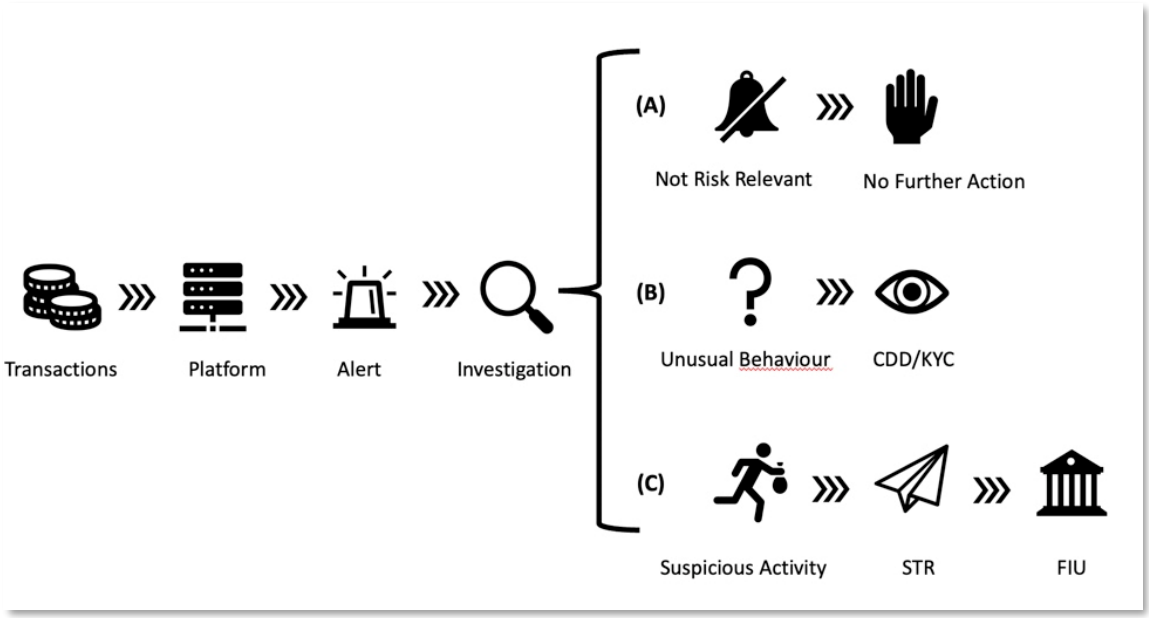
(4) the review of those cases by assigned investigators, leading to:

(a) the decision to take no further action, as the case can be concluded as not risk relevant

(b) send the case to a CDD team, or other relevant party, initiating a customer report based on the unusual behaviour detected; or

(c) send to a MLRO to file a STR

FIGURE 6 – Basic Monitoring and Reporting Process[28]



2.2 Manual and Automated Approaches

FIs' monitoring mechanisms use either manual, automated or combined processes. In the early years of the global AML regime, manual monitoring, either through dip sampling in branch, or via batch inspection in back office service centres, was commonly used by FIs to fulfil their obligations. The manual approach continues in many FIs with smaller transactional volumes, such as private banks and family offices, or DNFBPs such as lawyers and real estate agents, who have limited numbers of higher value transactions to review. However, across the market, the last two decades has witnessed a strong movement – even amongst smaller firms – towards increasing automation.[29]

[28] Author's own design based on research conducted for this study.

[29] Author interviews with: (No.1); (No.15) senior compliance professional based in US, (4 June 2020); (No.27) compliance consultant based in UK, (10 June 2020); (No. 29) senior TM specialist based in Hong Kong, (2 June 2020).

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. In the start-up world, many Financial Technology (FinTech) firms continue to express a preference for technological self-reliance,[30] but it is more usual now to see FIs buying in standard models from market-leading technology vendors.[31] In many cases, it is also not uncommon for FCC functions to run several different platforms, especially when the FI has multiple lines of business and/or operates in many jurisdictions. This growth in the deployment of automated platforms has thus had consequences for the scale of technical support necessary to undertake monitoring, often leading to the development of dedicated TM teams with FCC Technology functions, sometimes supported by vendors or management consultancies.[32] However, there are some FI products that are more difficult to monitor through automated systems, such as documentary Trade Finance, where little inroads have been made over recent years to identify effective tooling in this area, with many FIs and vendors exploring possible solutions.

2.3 Automated Monitoring Strategies

As shown in Figure 6 above, the TM process begins with the ingestion of transactional data from core internal payments management systems into the monitoring platform, most often through delayed periodic batches on a daily, weekly or monthly schedule. The platforms then apply structured approaches to the transactions of potential concern. There are two leading methods for achieving this at present:

- **Rules-Based.** Rules-based models apply combinations of rules (e.g. multiple payments up to a round figure, high volume and/or velocity, etc.) to transactions to identify potential matches of behaviour in the data.
- **Behavioural**. Behaviour-based approaches seek to identify whether client activity remains consistent with what is known about the client in CDD files or against peer groups within the same data set, although peer grouping is limited by the relevant reference data set within the FI. To achieve this, clients are typically also risk-ranked and grouped in segments to observe how individuals' behaviours compare with their peers.

Another method, which is often used by those in the virtual assets sector and in correspondent banking, focuses on counter-party risk, with systems monitoring for transactions with known or suspected 'bad actors', including accounts which have featured on criminal market places on the Dark Web. In the vast majority of cases, these methods are retrospective, with monitoring platforms being fed transactions data in batch, post-event. However, a small but growing number of FinTech businesses have sought to apply automated solutions in real-time, stopping payments on the basis of alerts and conducting investigations before funds are allowed to move further.[33] Other, innovative approaches are also emerging, which will be tackled later in the paper.

[30]Author interviews with: (No.3) MLRO based in the UK, (20 May 2020); (No.14) compliance consultant based in Singapore (5 June 2020); (No.20) RegTech vendor specialist based in the UK, (2 June 2020).
[31] Craig, Patrick, Jodie Forbes, Eamon Howard, Becky Marvell, Matt Reed, 'Anti-Money Laundering (AML) Transaction Monitoring: 2018 EMEIA Survey Report', *EY*, (October 2018), p. 13.
[32] Author interviews with: (No.9) senior TM specialist based in UAE, (11 May 2020); (No.29).
[33] Author interviews with: (No.3); (No.9) compliance consultant based in UK, (14 April 2020).

2.4 Detection Scenarios

Of the two main monitoring strategies, 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:

- **Unusual/Excessive Usage of Bank Services**, including online platforms, in-branch cash services, ATMs, etc.
- **Unusual Patterns of Funds Deposit and Withdrawal**, especially with regard to increased cash use, structured payments, and the use of dormant or semi-dormant accounts.
- **Unusual Patterns of Funds Transfer**, including variations of volume, value and velocity, recurrence of counterparties and circularity of payments.
- **Involvement of High Risk Factors**, including payments to high risk customers or jurisdictions, or use of branches in high risk areas.

In rules-based models, platforms may also include transaction value thresholds to remove lower value – and hence lower risk – transactions, and segmentation of client groups is increasingly common too, with thresholds for the application of rules varying depending on clients' risk profiles. Together, 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. Some rules-based platforms have additional capabilities to identify statistically significant changes in client behaviour, over time and their use in concert with rules-based approaches demonstrates some level of 'hybridisation'.[34]

2.5 AML Investigations

The application of detection scenarios within the platform leads to the production of alerts, which are then logged for investigation. In small FIs, this task can be fulfilled by the MLRO, but it is more common for FIs to have dedicated AML investigation teams. In top tier firms, there are three ascending levels, each exercising increasing degrees of scrutiny:

- **Level 1** is **Alert Assessment**, including the removal of obvious False Positives. Level 1 can close alerts or pass on to Level 2.
- **Level 2** is **Case Analysis/Investigation**, where the focus is on validating whether there are grounds for concern. These teams can also close alerts or pass to Level 3.
- **Level 3** is **Investigation and Reporting**. These teams conduct a more extensive investigation of the alerts remaining. These teams can close the case, pass to CDD for a client review, or provide recommendations to the MLRO regarding filing an STR.

The largest teams of investigators tend to be deployed in Levels 1 and 2, and in many cases, such teams are also located offshore from the jurisdiction. Level 3 investigators usually comprise the most experienced AML investigators, and will be located in the jurisdiction where a report might need to be made. Alerts are typically processed through an end-to-end investigative case management platform, but there can be significant variation between the range of investigative tools available to AML investigators at different levels. Level 1 and 2 have more limited options at their disposal, such as internal CDD systems or the Internet, although contacting clients or other banks through 'Requests for Further Information' (RFIs) can sometimes start at Level 2. Such

[34] Author interviews with: (No.4) panel of senior compliance and regulatory professionals, based in Hong Kong, (21 April 2020); (No.7) senior RegTech vendor specialist based in UK, (15 May 2020); (No.9); (No.11) compliance consultant based in UK, (14 April); (No.29).

options are also open to, Level 3 teams, which also usually have access to a wider range of internal and external data sources and analytic tools.[35]

2.6 Technical Support and Optimisation

The final element of a typical internal FI TM structure is technical support. Technical teams play an integral role in the creation of in-house platforms or the implementation and optimisation of vendor solutions, from the development of the necessary infrastructure, the sourcing of data, through to the initial phase of detection scenario configuration and testing. But more than that, they are essential to maintaining automated platforms throughout their lifecycle in a process commonly described as 'optimisation,' which involves testing and tuning the parameters of the platform to assess and manage risk coverage and alert volumes. Optimisation typically takes place on a regular annual, half yearly or quarterly basis, with end-to-end reviews of data quality and platform outputs. 'Back-Testing' is applied to identify alert volumes and 'hit' rates for different rules, and increasingly, FIs are also deploying 'Above-The-Line' (ATL) and 'Below-The-Line' (BTL) testing to tune threshold values, so as to assess the volume and quality of alerts that will be produced at different levels.[36]

2.7 External Stakeholders

TM and reporting functions are, part of a wider AML framework. The primary external channel on a day-to-day basis is the national FIU, which receives STRs or their equivalent. FIUs have different set-ups, from administrative offices to departments within LEAs or prosecutorial bodies. FIs' other key stakeholders are the national regulators charged with providing independent oversight of AML frameworks of FIs. Following FATF's Assessment Methodology, this comprises an assessment of technical compliance and how effectively policies, procedures and controls have been implemented.[37] For TM, a regulatory examination also includes reviews of platform risk coverage and performance, alert handling quality by investigators, and model governance and validation, confirming that the working of the platform is both explicable and repeatable.[38]

2.8 Conclusion

In summary, the development of TM in practice within the financial services industry shows significant commonality, with the increasing importance and deployment of automated platforms to undertake monitoring and AML investigators to process alerts. Indeed, the centrality of technology cannot be understated, and in many compliance professionals' minds now, TM is synonymous with the platform itself, rather than the underlying monitoring requirement; as one with thirty years experience, commented it is "difficult to remember back to a time before we used systems."[39] However, the burgeoning growth and sophistication of technology in TM has not removed the need for human support. Platforms need to be configured and alerts worked, tasks which still require significant human input at this point. As we shall see, however, these tasks are not without challenges.

[35] Author interviews with: (No.1); (No.10) senior compliance specialist based in Sweden, (30 March 2020); (No.29).
[36] Author interviews with: (No.4); No.(9); (No.29); (No.31) senior TM specialist based in Singapore, (19 May 2020).
[37] FATF, 'Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems', (Revised February 2019), p.104.
[38] See, for example: US Federal Financial Institutions Examination Council (FFIEC), 'Bank Secrecy Act/ Anti-Money Laundering Examination Manual', (2014).
[39] Author interview (No.7).

3 – TM Challenges

Implementing any Information Technology (IT) solution is a major project, and TM platforms are no exception. 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 TM because of the multiple demands that are placed upon it: not only to provide financial intelligence, but also to meet internal cost *and* external regulatory requirements. These conflicts become most obvious when platforms are configured and reporting thresholds set, when finding a satisfactory balance between competing demands – what one TM specialist called "the Goldilocks zone," – can be difficult to achieve.[40]

3.1 Selecting Platforms

In some smaller FIs, especially amongst the start-ups of the FinTech world, there are examples of TM platforms being developed quickly by in-house teams in a matter of weeks, partially enabled by limited product variations and fewer legacy systems. However, in the mid-tier and upwards, the decision-making around what kind of platform to have – whether to self-build or use a vendor, or which vendor to use, can take many months to accomplish. The larger the FI, the more internal stakeholders need to be involved or satisfied; functionally, that often includes a variety of risk teams such as Vendor Risk Management and Information Security, and for international businesses, it can also include engagement of regional and global levels of management. The outcomes of these discussions can often be influenced by internal politics, organisational frictions, pre-existing vendor relationships, line of business specific requirements related to monitoring and variable levels of technical, legal or cultural understanding amongst senior decision-makers.[41]

3.2 Building Platforms

Once a decision has been made, the process of implementation is usually multi-staged, from initiation, planning, execution, testing, to closure. This process can last anywhere between six months to over a year depending on the platform and the complexity of the FI, and occasionally longer, depending on how many obstacles are encountered along the way. As with any IT project, there can be basic issues with ensuring ongoing senior management commitment if timescales and budgetary requirements expand beyond expectations. TM implementations also typically face a consistent set of practical problems, especially during planning and execution:[42]

- **Poor Data Access and Quality:** In most circumstances, TM platforms are implemented within the context of a mature business, where transaction data is stored within several separate core payments systems located within different parts of the FI. As a senior US compliance specialist explained, in many large and mature FIs, TM programmes are thus confronted with a "Balkanised legacy of multiple data sets and systems," which are difficult to access, connect and harmonise.[43] The older the systems, moreover, the greater the issues with respect to detail, data quality, gaps and duplications, tend to be.[44]
- **Archaic IT Architectures:** TM platforms have to be implanted into extant IT structures, which, when more mature and complex, can be difficult to understand and navigate.

[40] Author interview (29).
[41] Author interviews with: (No 7); (No 8) senior compliance technology expert based in the UK, (15 May 2020); (29).
[42] Author interviews with: (No 7); (No 8); (No.20); (No.29).
[43] Author interview (37).
[44] Author interviews with: (No 7); (No 8); (No.20); (No.21) senior RegTech vendor specialist based in the UK, (20 May 2020); (No.29).

Many FI architectures have been developed by individuals who have long since left the business, and there is often no 'central view' of how all relevant systems work together. In some instances moreover, there are problems of poor compatibility between new TM platforms, with vendors expecting a globally consistent set of detailed high quality data and simple architectures.[45]

- **Lack of Technically Skilled Staff**: TM implementations increasingly rely on the deployment of a relatively rare body of technical talent. The more advanced technology becomes, the more specialised, scarce and therefore costly the technical skills required. Many specialists are reported to be highly paid, and at the top end of the market can earn more than the FCC executives who manage them.[46]

3.3 Configuring Platforms

Following its basic build, the configuration and testing of the platform's detection scenarios are further painstaking tasks. As noted previously, there are typically several streams of information shaping this process, including the firm's EWRA – which elucidates the financial crime risks the firm is likely to face – to 'known' typologies used in previous platforms and other occasional material on criminal activities produced by FATF, LEAs and other reputable bodies. Using this material, financial crime risks are prioritised, scenarios designed and parameters set. During pre-launch testing, these scenarios are then extensively back-tested against historic data, with threshold parameters tuned to balance coverage, False Positives and volumes.[47]

No matter how rigorous this process of configuration, however, it is an ambiguous and uncertain task where there is no accredited 'right answer.' FCC teams typically lack systematic guidance from FIUs and LEAs on criminal typologies, feedback post filing, or on what kind of financial intelligence would be most useful or relevant to their investigative priorities. The result, therefore, is that configuring scenarios can largely be a matter of informed guesswork based on historic data points, experience and professional judgement. As a long serving TM specialist remarked, it can often feel, in practice to be "a shot in the dark."[48]

Configuration can be shaped by other factors too, not necessarily directly linked to financial crime risk concerns. National and institutional AML cultures can affect the scope of risk coverage attempted by platforms; some, such as FIs in the US, tend to take a more expansive approach with a large number of scenarios and wide parameters, encouraged by an assertive regulatory culture. Others, such as those in Switzerland, for example, are far more targeted.[49]

3.4 Maintaining Platforms

Setting up TM platforms takes substantial effort, but that effort cannot end at 'go live.' The platform's data inputs, processes, and outputs, need to be kept under regular review, not least because TM is a major source of reporting that underpins FI's statutory obligations in that regard, but also because shifting economic, financial or financial crime risk environment can affect patterns of client behaviour. Some FIs found, for example, that the COVID-19 pandemic caused a

[45] Author interviews with: (No 7); (No 8); (No.20); (No.29).
[46] Author interviews with: (No 7); (No 8); (No.13) senior data engineer based in UK, (29 April 2020); (No.20); (No.21); (No.29).
[47] Author interviews with: (No 7); (No 8); (No.9); (No.13); (No.20); (No.21); (No.29); (No.31).
[48] Author interview (No.29).
[49] Halliday, Terence, Michael Levi and Peter Reuter, 'Can the AML system be evaluated without better data?', *Crime, Law and Social Change,* (March 2018), Volume 69, Issue 2, p.19.

steep decline in the activation of cash-based indicators and an increase in cases linked to 'unusual' patterns of digital activity.[50]

Running scheduled optimisation processes described in the previous chapter, or even mounting event-driven reviews outside of schedule, bring the same basic challenges as those that come with initial configuration of the platform. In smaller FIs, these can be a relatively straightforward exercise, but the larger and more international the FI in question, the more difficult the process becomes because of the need to involve multiple stakeholders' requirements, and meet business-wide standards. Experienced TM specialists in Europe and Asia-Pacific suggested that the technical elements of optimisation – the application of back-testing, ATL and BTL and the calibration of the impact of changes to alert volumes– could be accomplished within a month, but that the procedures for making approval dependent changes to platforms could take two to three months because of the need for various review cycles and management structures to agree, as well as to ensure that regulatory model validation requirements are met.[51] In the words of one of those specialists, "changing the platform is the easy part. Herding the cats is the difficult bit."[52]

3.5 Replacing Platforms

As the preceding discussion suggests, if the process of reconfiguring an existing platform can be problematic, the decision to demise and replace one will be a major undertaking, even when there is substantial dissatisfaction with an existing solution or a desire to innovate. The larger and more complex the business, the more difficult and costly change becomes. A senior IT expert who works for an international bank remarked that even when decisions are made, "attempts to rationalise or replace old systems can run aground because of the scale of the task and the unforeseen technical problems change brings." New implementations can thus "become very messy indeed," and in the worst case scenarios, businesses can "end up with a mix of different platforms, some only partially developed or jerry-rigged to work with what is already there."[53]

Change is not cheap either, and as regulators require coverage to be continuous, existing platforms have to continue to run alongside those under development. It often remains an open question how regulators will respond to the situation if a new TM platform identifies patterns that the previous platform did not, creating the need for extensive multi-year lookbacks, and adding to transition costs and risks. For smaller FIs with limited funds at their disposal, this can be particularly prohibitive. Reviewing these challenges, a former US MLRO commented that, for many FIs, the idea of "making do with what you've got" becomes an attractive option, especially when considered in the light of all the other challenges FCC teams face. "Most MLROs are only in position for a few years now," he remarked, "and they often spend their time on a succession of 'crises of the day.' Expecting them to use their capital on reforming TM is a big ask."[54]

3.6 Managing AML Investigations Teams

Platforms are, of course, not the only element in the TM framework. As outlined previously, the standard approach to TM involves the deployment of several echelons of AML investigators to handle alerts. Recruitment into the larger Level 1 and 2 teams typically focuses on finding intelligent but relatively cheap labour – often new graduates in offshore locations – to validate

[50] Author interviews with (No.11); (No.60), MLRO based in the UK, (25 March 2020).
[51] Author interviews with: (No.13); (No.20); (No.29).
[52] Author interview (No.29).
[53] Author interview (No.8).
[54] Author interview (No.47).

alerts or decide whether there is value in further investigation at a higher level. This can often become a routinised and formulaic activity where sensitivity to potential risk declines over time. As a former AML investigator remarked, the experience of working in a Level 1 team was "like drinking from a fire hose," with the management focus being on "volume and throughput."[55] Low staff morale and high attrition rates often result, impacting quality of the risk management.[56]

At Level 3, the needs are, of course, different. Here, FIs tend to recruit specialised staff, often with previous investigative training and experience in law enforcement, the military or intelligence. Although perhaps less rare than technical staff, such individuals are still relatively limited in number, and there is a strong emphasis on recruiting and retaining those who can demonstrate good investigative judgement. Nonetheless, even for those experienced in investigatory techniques, AML provides its own difficulties. Much like the configuration of detection scenarios, the investigation of transaction-based alerts can be hampered by the variable nature of what 'suspicion' is thought to look like in transactions data. At Level 3, investigators usually have more time to review other internal and external sources to form a judgement, but this is still a narrower range of material than most public sector investigations are able to exploit, and the investigator invariably runs up against institutional data barriers in complex cases with extensive links to other jurisidictions and FIs, where strict data privacy laws can apply.[57]

The uncertainty around standards of suspicion make decision-making difficult to execute with confidence. Significant ambiguity is inherent in such a decision, and alongside the personal biases of the investigator, institutional risk attitudes about whether a 'smoking gun' or a pattern of behaviour consistent with suspicion is required will help shape the outcome.[58] For those under current or past regulatory pressure, this can further skew the outcome towards defensive reporting, for the simple reason that, as intelligence academic Michael Herman has written "underestimation is less readily forgiven than overestimation."[59]

3.7 Conclusion

The development and management of TM platforms has thus presented FCC functions with a complex set of interconnected and ongoing challenges. Platforms need to be configured, investigators trained, and reporting thresholds set, not only to meet the reporting requirement, but to satisfy regulators' risk coverage requirements and internal cost constraints. Balancing these demands to a point where FCC teams are not subject to regulatory or internal criticisms might be seen as an achievement of sorts. However, there is a danger that if finding that balance becomes the sole focus of a TM and reporting framework, then the central rationale behind both, identifying valuable financial intelligence, might be lost in the process.

[55] Author interview (No.40) former senior FI AML investigator based in the UK, (11 June 2020).
[56] Author interviews with: (No.1); (No.3); (No.9); (No.40).
[57] Author interviews with: (No.3); (No.8); (No.10); (No.21); (No.40); (No.55) former senior investigator based in UK, (29 June 2020).
[58] Author interview (No.10).
[59] Quoted in Clark, Robert M., *Intelligence Analysis: A Target-Centric Approach*, 6th Edition, (Sage: London, 2020), p.109.

4 – TM Outcomes

The AML world is increasingly focusing on the question of 'outcome effectiveness': whether the policies of the past three decades have led to an appreciable improvement in financial crime disruption and thus to 'impact effectiveness' – a reduction in illicit flows.[60] However, even though TM and its linked processes should play a vital role in supporting both, the data to demonstrate this is patchy, showing high percentages of low quality alerts and unused STRs. This might be partly the result of poor implementation at individual FIs, but at a strategic level, it is more likely to be a natural consequence of the difficulty that private institutions have in recognising and tracking financial crime confined within the scope of their own transactions in a given jurisdiction. Debatable intelligence benefits come, moreover, with clear costs and externalities. FI expenditures on the components of the TM model continue to rise, and regulatory scrutiny is progressively more intense despite the lack of improved performance. In TM, therefore, the financial services sector have found themselves in the unenviable position of running a costly and risk-laden control, where the potential for success is limited at best.

4.1 Quality Metrics

In other contexts where intelligence is produced, such as national security or law enforcement, the material's effectiveness is typically assessed by its recipients on criteria such as reliability, accuracy, timeliness, relevance and operational utility.[61] Similar feedback mechanisms are largely missing in AML, however, and FIs are largely dependent on self-created metrics to assess their intelligence production performance. The two most commonly cited across the industry are:[62]

a) **The False Positive (FP) Rate:** The proportion of alerts deemed neither unusual or suspicious by AML investigators. This is treated as a rough-and-ready measure of platform accuracy.
b) **The Suspicious Transaction Report (STR) Conversion Rate**: The proportion of alerts that lead to an STR. The figure is used to estimate 'True Positives' produced by the platform.

FP rates vary somewhat between business lines, FIs and geographies. However, industry data from a range of sources suggest that the typical proportion of FPs is high, with even the lowest figures suggesting over two thirds of alerts are FPs.

Source	FP Rate
PwC, 2010	**90-95%**
Bain and Company, 2018	**90%+**
Ernst and Young, 2018	Capital Markets: **85%** Wealth Management: **85%** Retail: **76%** Corporate: **69%**
McKinsey and Company, 2020	**90%**

Table 1: False Positive Rate Industry Estimates[63]

[60] Redhead, Matthew, 'Deep Impact? Refocusing the Anti-Money Laundering Model on Evidence and Outcomes', *RUSI Occasional Paper* (October 2019), pp.11-15.
[61] Author interviews with: (No.8); (No.10); (No.21); (No.28) senior law enforcement officer, based in the UK, (12 June 2020).
[62] Author interviews with: (No.7); (No.9); (No.29); (No.34), senior RegTech vendor specialist based in the UK, (12 June 2020); (No.42) senior AML consultant panel, based in Hong Kong, (18 June 2020).
[63] Craig, Patrick, et al, 'Anti-Money Laundering (AML) Transaction Monitoring: 2018 EMEIA Survey Report', p.5; Giacomini, Paul, Marco Iacano, Jeff Levine, Thomas Messina, Nathan Thomas, 'From Source to Surveillance: The Hidden Risk in AML Monitoring System Optimization', *PwC*, (September 2010), p.1; Hayday, Matthew Jan-Alexander Huber, Matthias Memminger, Michael Soppitt, 'How Banks Can Excel in Financial Crimes Compliance', *Bain and Company*, (18 January 2018), https://www.bain.com/insights/how-banks-can-excel-in-financial-crimes-compliance/, accessed 1 October 2020; Murphy, Adrian, Kate Robu, and Matthew Steinert, 'The Investigator-Centered Approach to Financial Crime: Doing What Matters', *McKinsey and Company*, (May 2020), p.10.

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

Amongst those interviewed for this study, estimates were along similar lines. The most quoted range for FPs was around 80-90% for conventional TM platforms, with STR conversion rates in the region of 2-10%, figures which appear to have remained largely the same for several decades. [64] There were a handful of significant outliers, with two compliance professionals suggesting they had seen STR conversion rates of 20-30% range from conventional TM solutions,[65] but even with these examples taken into account, the weight of available evidence paints a largely negative picture. The numbers deteriorate much further, moreover, when STR rates are put into context of the total number of monitored transactions, when the conversion rate transactions to STR will drop below 0.005%.

4.2 Outcome Metrics

Measures for the intelligence outcomes TM alerts bring are also limited. Figures for STR usage tend to be largely anecdotal 'guesstimates' by law enforcement officials, as FIUs and LEAs do not typically trace how STRs are used.[66] Even so, the material available is not encouraging. In a 2017 survey, Europol, the EU's policing agency, found that only 10% of STRs received by FIUs in the Union were likely to have immediate investigative value, with the vast majority of reports filed for secondary usage at a later date.[67] More recently, in interviews conducted for a 2019 study by the Royal United Services Institute (RUSI), a security think tank, former senior law enforcement officials provided lower estimates still for immediate STR usage, of between 1-2%.[68] If these figures are anywhere near correct, they suggest that FIs' TM efforts are having a small impact on law enforcement investigations.

There is no agreed benchmark for 'good' or 'bad' TM platform performance, but from an absolute perspective, any end-to-end intelligence production process which generates mostly unusable or unused material is open to question. Relative to other forms of alerts, moreover, the figures also seem poor. Several interviewees drew comparisons with staff alerts generated by front office personnel (also referred to as 'manual TM'), where FPs are much more rare due to initial 'sense checking' by staff, and conversion rates to STR are estimated to be between 50-60%. Despite the overall low usage of STRs, several law enforcement officers and regulators further suggested that STRs which resulted from staff-triggered alerts had more value than TM-based alternatives, because of the investigative detail they provided.[69]

[64] Author interviews with: (No.3); (No.7); (No.9); (No.10); (No.14); (No.15); (No.21); (No.22) senior AML consultant based in the UK, (24 April 2020); (No.23) senior compliance official based in the US, (14 May 2020); (No.27); (No.29); (No.30) senior compliance officer panel based in Spain, (19 May 2020); (No.31); (No.33) senior compliance officer based in the US, (12 June 2020); (No.36) MLRO based in the UK, (1 July 2020); (No.37); (No.42); (No.47); (No.58) AML journalist panel based in the UK, (20 Match 2020); (No.60).
[65] Author interviews with: (No.1); (No.20).
[66] Author interviews with: (No.25) senior civil servant based in the UK, (10 June); (No.28); (No.40); (No.47).
[67] Europol, 'From Suspicion to Action: Converting Financial Intelligence into Greater Operational Action', (2017), p.4.
[68] Redhead, Matthew, 'Deep Impact?' *RUSI Occasional Paper*, p.16.
[69] Author interviews with: (No.1); (No.4); (No.5) senior compliance professional based in the UK, (5 May 2020); (No.19) senior compliance professional based in the UK, (3 June 2020); (No.36); (No.37); (No.38) senior compliance professional panel based in Singapore, (16 June 2020); (No.47); (No.58).

4.3 Explaining the Metrics

In some instances, the high volume of low quality TM alerts might be attributed to poor management of TM platforms within FIs. In its recent industry guidance on TM, the Monetary Authority of Singapore (MAS), the jurisdiction's AML regulator, found that many FIs had no scheduled regimen for reviewing platform settings, and a RegTech specialist, interviewed for this study, commented that he regularly visited mid-tier FIs who had "assumed that 'factory settings' were all they needed."[70] This kind of laissez-faire approach undoubtedly pushes up FP rates in individual FIs. In many others, the day-to-day challenges and frictions of running a TM framework, touched upon in the previous chapter, will also have an impact. Inherited legacy platforms and data, limited staff resources or inflexible management structures can all hamper performance. However, these factors, even in concert, are unlikely to be the root cause of TM's bias towards waste.

In fact, the problem is likely to be inherent to the task itself. Although the FATF Recommendations state that obligated entities should monitor for consistent behaviour alone, and the majority of sampled national laws accord with this, the industry approach to TM is predominantly focused on finding patterns of illicit activity in transactions data: a much more difficult task than the (still challenging) problem of identifying inconsistent transactions against a baseline of expected behaviour. While FIs mostly 'know their customers', they do not know *definitively* how criminals launder funds or what financial criminality looks like in transactions data. What currently passes for industry knowledge is vague and largely unconfirmed; as a senior European TM and AML investigation specialist commented, "the truth is, you just don't know. This isn't like a sanctions hit or a fraud. With sanctions, you can confirm it or discount it. With fraud the customer rings you up. There's a feedback loop. But launderers don't leave a calling card."[71]

Overlaid on top of this ambiguity is the further fundamental difficulty of identifying distinct patterns in data. Any monitoring strategy can take one of two approaches: cast the net wide and apply only a small number of criteria to identify a criminal typology, or 'spear-fish' with very detailed parameters.[72] In the first approach, a great deal of activity will be identified, but a high proportion will likely be innocent; in the second approach, a very small number of alerts will result, but significant amounts of potentially concerning activity will be probably also be missed. The execution of the task is hindered drastically, moreover, by the limited scope of data available to individual FIs due to data privacy constraints, which hamper data sharing within FIs, and make it extremely difficult both between FIs, and between FIs and public sector agencies. Indications of concern might well exist within transactions data, but these can be distributed across the datasets of multiple FIs, and also in official databases. The more dispersed the criminal activity, the greater the risk of its invisibility.

The basic challenge of detecting illicit activity via platforms is also mirrored in the process of AML investigation and STR production. Human failings play their part, and regulators such as MAS have reported examples of weak investigative practice at FIs.[73] Law enforcement officials also report from many jurisdictions that STRs can be of variable quality.[74] Nonetheless, asymmetries of knowledge and a fragmented view of the data can hinder human investigators too. Only criminals fully understand their own *modus operandi*, and the more complex and multifaceted their techniques, the less detectable they are; expecting AML investigators to be able to achieve this

[70] Author interview (No.34).
[71] Author interview (No.10).
[72] An expression originally coined by one of the reviewers of the paper, unneknown to the author when used.
[73] Monetary Authority of Singapore (MAS), 'Guidance for Effective AML/CFT Transaction Monitoring Controls', (September 2018), pp.12-13.
[74] Author interviews with: (No.28); (No.40); (No.49) former senior law enforcement official based in the UK, (4 June 2020).

without the range of privileged sources available to law enforcement is unrealistic. And despite their poor reputation, STRs are not all of low quality. Sometimes, their exploitation reflects a lack of relevance to immediate LEA priorities, or other public sector weaknesses, such as FIUs' limited resources in the face of increasing STR numbers, poor technical capabilities and training. In theory, therefore, a larger proportion of STRs could be of value if there were better feedback loops between the public and private sector, and closer alignment between what LEAs required, and FIs produced.

4.4 Costs

If the benefits of TM are hard to demonstrate, the costs are not. A 2020 study by the legal information provider, Lexis Nexis, indicates that the total cost of FCC programmes across around 14,000 FIs in the key markets of Asia-Pacific, Europe, the Middle East and Africa, and the Americas, is around $180.9 billion, most of which is being spent in Europe and the US.[75] Of that, TM-related activities are likely to take a large proportion. A previous study by Lexis Nexis in 2017 suggested that monitoring and reporting probably accounted for around 30% of overall FCC costs.[76] This suggests a current TM-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 in industry estimates, with figures ranging from around 60 to nearly 80%.[77] Senior compliance officials interviewed for this study indicated that a similar pattern was mirrored in spending of monitoring and reporting, with a high proportion of personnel costs devoted to AML investigatory teams.[78] One TM specialist from a leading vendor estimated that over 90% of the cost of an alert was typically related to its handling, rather than its production. Although this proportion could vary depending on the volume of alerts, the total number of investigators and the time taken to complete an individual alert, it was commonly a high figure.[79]

4.5 Regulatory Risks

As a core AML control, TM frameworks are also a major focus of regulatory attention, and as outlined in Chapter 2, regulators are tasked to identify an FI's technical compliance and make a subjective evaluation of how well they have implemented their solution. However, as a former MLRO commented, TM frameworks can "only ever be satisfactory at best," and as consequence, are a consistent target of censure.[80] A 2020 analysis by legal firm Duff and Phelps found that between 2015 and 2020, 22% of regulatory fines in the US, Europe and Asia-Pacific related to failures in monitoring and reporting.[81] Many of these relate to the poor management of TM platforms, ranging from insufficient attention to platform configuration, irregular and undocumented optimisation, unresolved technical issues with data, and a failure to keep risk

[75] Lexis Nexis Risk Solutions, 'True Cost of Financial Crime Compliance Study: Global Report', (March 2020), p.6.
[76] Lexis Nexis Risk Solutions, 'True Cost of Financial Crime Compliance Study: European Version', (September 2017), p.9.
[77] Bevan, Oliver, Piotr Kaminski, Ida Kristensen, Thomas Poppensieker, and Azra Pravdic, 'Compliance at an Inflection Point,' *McKinsey and Company*, (January 2019), p.7;
Lexis Nexis Risk Solutions, 'True Cost of Financial Crime Compliance Study: Global Report', (March 2020), p.13; Lexis Nexis Risk Solutions, 'True Cost of Financial Crime Compliance Study: European Version' (September 2017), p.9;
[78] Author interviews with: (No.3); (No.8); (No.11); (No.17) former MLRO based in the UK, (3 June 2020); (No.22); (No.27); (No.42); (No.47); (No.60).
[79] Author correspondence with: (A) RegTech vendor specialist based in UK, (September 2020); (B) data engineer based in Denmark, (September 2020).
[80] Author interview (No.47).
[81] Bayley, Nick, '2020 AML Fine Values Already Surpass 2019 as Firms are Repeatedly Sanctioned for the Same Failings' *Duff and Phelps*, (10 August 2020), https://www.duffandphelps.com/about-us/news/duff-phelps-global-enforcement-review-2020-launched, accessed 10 September 2020; Jakubowski, Zak, 'Global AML fines reach £540m with reoccurring failures', (10 August 2020), https://www.accountancydaily.co/global-aml-fines-reach-ps540m-reoccurring-failures, accessed 10 September 2020.

segmentation up-to-date, as well as some instances of inefficient or insufficient AML investigation. Such fines continue to impact major FIs, including even those that have previously been censured and have invested to improve their TM programmes.

Mistakes and failings by FIs contribute to these problems, as do the broader challenges of seeking to make many moving parts within the TM framework work together. Escalating costs also play a role. The heavy imbalance between technology and investigatory costs means that it is common practice across the sector to try to attain an acceptable balance between False Positives, alert volumes and risk coverage during optimisation.[82] In some instances, however, this goes too far for regulators, especially if FIs appear to be intentionally limiting numbers of alerts to reduce costs. In US actions, banks have been fined by the Financial Crimes Enforcement Network (FinCEN), the US FIU, for seeking to cap the number of TM alerts to workable levels for existing AML investigator numbers. FinCEN has noted how the specific narrowing of thresholds settings in bank TM platforms had led to a failure to identify suspicious activity that should have been reported.[83]

4.6 Conclusion

TM and reporting frameworks as they have evolved over the last three decades are thus now in serious difficulties. High volumes of wasted alerts, wasted investigative effort, and little discernible value-add to the broader fight against financial crime, combined with escalating costs and regulatory censure, bring the issue of TM reform 'front and centre' for FIs and the wider AML ecosystem. As currently implemented, TM has lost sight of its initial objective: to generate useful intelligence for LEAs that can help identify and stop money laundering and – through a concerted effort – reduce the amount of illicit funds in the financial system. To many practioners, these problems are now perceived as existential, and in the next chapter, we go on to explore some of the ways in which key players are seeking to deal with them.

[82] Author interviews with: (No.1); (No.9); (No.11); (No.15); (No.22); (No.23); (No.30); (No.33); (No.37); (No.42); (No.47).
[83] US Treasury Financial Crimes Enforcement Network (FinCEN), 'FinCEN Penalizes US Bank Official Corporate Anti Money Laundering Failures', (4 March 2020), https://www.fincen.gov/news/news-releases/fincen-penalizes-us-bank-official-corporate-anti-money-laundering-failures, accessed 10 March 2020.

5. TM Innovation

FI initiatives have provided the primary impetus for TM reform, at first inspired by a succession of regulatory actions against major institutions, but increasingly, a positive desire from the industry to make TM more effective in delivering anti-financial crime outcomes. Over the last decade, much resource and effort has gone into the upgrading of platforms and investigatory capabilities, as well as supplementing transaction-focused processes with other forms of risk management. Although many regulators have maintained neutrality towards innovation, several leading bodies have openly encouraged it, and FIUs and LEAs have also engaged with FIs through Financial Intelligence Sharing Partnerships (FISPs).

Initial evidence on the impact of these reforms is limited and anecdotal, but broadly positive, and in most cases, initiatives could be profitably taken further. FISPs, for example, could play a greater role in the more effective configuration of TM platforms. But innovation brings its own challenges, and not all initiatives are workable across the entire sector. Even if they were, moreover, their effects would be limited because of the ongoing fragmentation of the AML ecosystem, leaving much illicit activity undetected in the gaps of coverage between FIs.

5.1 FI Reforms

FIs have focused chiefly on TM platforms, with improved optimisation regimes and the deployment of data-driven technologies. But there have also been attempts to professionalise AML investigatory teams and enhance their technological capabilities, as well as experimentation with broader forms of risk monitoring, both within the business and in newly created intelligence and analytics functions.

5.1.1 Platform Improvements

At the most basic level, FIs have begun to look again at how they use their existing TM platforms, with FIs gradually becoming more rigorous in the application of the capabilities they already possess. One TM vendor specialist commented that he had seen several examples of FIs seeking to "work the system harder," by ensuring that they were responding at speed to changes in the risk environment, such as during the early stages of the COVID-19 pandemic.[84] What this means in practice is an increasing tempo in optimisation, 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.[85]

A further common initiative is the deployment of new technologies, either to enhance or replace existing platforms, especially amongst top and mid-tier FIs. Increased computing power from distributed networks known as 'Cloud' computing, combined with vast amounts of data from the increasing digitisation of economies and societies, have made industrial-scale analytics technologically and financially feasible in a way that was inconceivable even in the recent past.[86] The deployment of these tools in the AML space is advancing amongst FIs, although it is still far from universal. According to a 2018 survey by the International Institute of Finance (IIF) and the

[84] Author interview (No.34).
[85] Author interviews with: (No.1); (No.13); (No.29); (No.34).
[86] Adams, Heather, Saad Choudri, Philippe Guiral and Samantha Regan, 'Evolving AML Journey: Leveraging Machine Learning within Anti-Money Laundering Transaction Monitoring', *Accenture Consulting,* (2017)'; Craig, Patrick, Aaron Gross, Matthew Reed and Rafael Pontes (EY), 'Advanced risks, advanced opportunities?', *inCOMPLIANCE* Issue 29 (May 2017), pp.34-36; Craig, Patrick, Mark Gregory and Tom Salmond, (EY) 'Financial Crime 2.0', *inCOMPLIANCE* Issue 33 (March 2018), pp.25-28.

professional services provider Deloitte, 34% of the FIs surveyed were actively using new analytical techniques for AML purposes, 35% were experimenting, whilst 31% had plans to do so in the future.[87] Of these new technologies, two are now in regular use within TM platforms:

- **Robotic Process Automation (RPA),** which uses software robots (known as 'bots') to undertake pre-programmable repetitive tasks and behaviours at high speed;[88] and
- **Machine Learning**, a field of Artificial Intelligence (AI) which uses learning algorithms to analyse and categorise data. Unlike conventional static formulae, these algorithms have flexible parameters that can change in response to what they find in the data they process, allowing the algorithm to identify patterns and make predictions on that basis.[89] The field is 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 (UML),*** which identifies patterns across unlabelled data, with the algorithm creating its own categories based on clusters of apparent commonality.

Together, 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 both ATL and BTL testing to assess the productivity of detection scenarios based on previous cases that have been concluded by its AML investigators.
- **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 FPs. In some instances, this can also include the closure of alerts deemed to be an FP by the algorithm.

Although less common, SML has also been used more directly in its own right as a method of categorising different known typologies in transactions data, or to identify consistent versus inconsistent client behaviours within different risk segments. A relatively small number of FIs appear to have been experimenting 'offline' with the more advanced technique, UML, applying it to many of the same tasks such as segmentation, or the identification of variations in client segment – and in some cases individual client – behaviours. UML has also been tested as a method of doing what SML cannot do – identifying new and previously unknown clusters of behaviour and/or relationships in transactions and other data.[90]

The initiatives outlined above are all relatively novel, and therefore most of the evidence with regard to impact – although promising – is anecdotal and difficult to verify fully. Firstly, the potential value of agile platform optimisation is strong in theory, and several TM specialists argued in interview that conventional platforms would attain better results if they were reconfigured more diligently and frequently.[91] One head of TM for a European FI stated that regular platform optimisation helped their institution achieve STR conversion rates of over 30%,

[87] International Institute of Finance (IIF), 'Machine Learning in Anti-Money Laundering – Summary Report' (2018), p.2, p.31.
[88] Association of Intelligent Information Management (AIIM), 'What is Robotic Process Automation?', https://www.aiim.org/What-is-Robotic-Process-Automation, accessed 1 October 2020.
[89] Domingos, Pedro, *The Master Algorithm,* (London: Penguin Books, 2015), pp.1-22.
[90] The examples above come from author interviews with: (No.7); (No.8); (No.13); (No.20); (No.21); (No.29); (No.38); (No.42); (No.60).
[91] Author interviews with: (No.1); (No.10); (No.21).

even using a rules-based platform.[92] However, consistent quantitative evidence of this type has not emerged, and several compliance officials questioned whether such an approach would work easily in larger and multinational FIs. In larger groups, complexity is increased by many and differing jurisdictions, organisational structures, diverse products types and client segments, and platform changes are likely to bring about intense regulatory scrutiny with regard to model risk management.[93] At this point therefore, the value of high intensity optimisation requires more solid evidence of material impact and workability.

There is more evidence on the potential impact of new technology, which appears encouraging. Interviews with both vendors and compliance professionals suggest that the application of RPA and SML to the pre-exisiting alerts produced by rules-based platforms can have a marked impact on FP rates, with 40-50% reductions possible.[94] An experienced AML regulator also suggested that SML techniques could be adept at identifying simpler patterns of behaviour in the early stages of money laundering, when illicit funds are 'placed' and initially 'layered' in the financial system.[95] This is an important distinction, as it suggests some capability to discover new and previously undiscovered patterms.

Nonetheless, the rough halving of FP rates still leaves those rates relatively high, and SML's recognised capability in classifying some patterns of behaviour is reportedly more difficult to replicate for complex typologies.[96] Emerging new criminal behaviours are also largely beyond its scope, and this is where some RegTech specialists believe that UML will fill the gap. Experimental findings do indeed suggest that clustering techniques can provide new insights into previously unseen patterns of transactional behaviour, but as one specialist commented "without further work, you will not be able to say whether it is suspicious." Human adjudication would thus continue to play an important role. As the specialist further explained, while UML has the potential to find previously buried False Negatives, it could also well produce "a whole new batch of False Positives."[97]

The deployment of these new technologies does not come without difficulties either. Assembling the right combination of in-house talent, technological know-how and appropriate computational capacity to install new platforms can be costly. In a 2018 report, professional services provider Accenture found that of the FIs it surveyed, 76% saw a gap between technical skills needed for AML innovation and those available on the open market.[98]

Even with funds, time and good quality staff on their side, moreover, innovating FIs 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,[99] which can prove a problem for FIs of all sizes and types. Smaller and more recently established FIs have better quality and more accessible material 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.[100] 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 large data sets leveraging private (in-house) or

[92] Author interview (No.1).
[93] Author interviews with: (No.7); (No.8); (No.29).
[94] Author interviews with: (No.7); (No.8); (No.11); (No.12) RegTech TM specialist based in London, (30 April 2020); (No.13); (No.20); (No.21); (No. 32), RegTech consultant panel, (11 June 2020); (No.38).
[95] Author interview (No.38).
[96] Ibid.
[97] Author interview (No.20).
[98] Besbes, Nesrine, Rafael Gomes, Samantha Regan, Ben Shorten, '2018 Compliance Risk Survey: Comply and Demand', *Accenture Consulting,* (2018), p. 3.
[99] Domingos, Pedro, *The Master Algorithm,* (Londo2015), pp.1-22.
[100] Author interviews with: (No.3); (No.7); (No.8); (No.11); (No.13); (No.20); (No.21); (No.29); (No.34); (No.42).

external (hosted) clouds. Attractive solutions though data lakes are in theory, however, they have proven to be long-term 'mega-projects' in their own right, even for extremely well-resourced FIs, and prone to major technical barriers and data-sharing issues between jurisdictions with differing data laws. These factors have tended to mean that so far, new technologies, though often sold to senior FCC leaders as cost savers, have rarely turned out to be more than cost neutral in the best cases, and have mostly led to short-term cost increases.[101]

Finally, programmes also face a current regulatory requirement to run in parallel with existing systems – another cost – until FIs can feel confident that the 'switch' between the two will not have deleterious results on coverage, or bring criticisms from regulators. From the regulator's perspective, machine learning brings with it particular issues with regard to transparency and model validation; all platforms should have an easily auditable logic and should produce the same result in the face of the same data. This does not pose major difficulties for techniques such as RPA, and even many styles of SML, such as 'Decision Tree' algorithms, can be relatively easily explained because of their roots in human thinking patterns. But the behaviour and outputs of UML algorithms typically defy human explanation or repeatability, and at present, regulators have no widely accepted technique for validating UML results. Most regulators are thus shying away from broadly endorsing UML platforms until wider societal decisions are made on the use of such tools in general.[102] Global initiatives such as the Institute for Electrical and Electronics Engineers' (IEEE) 'Global Initiative on Ethics of Autonomous and Intelligent Systems,' and the 'Partnership on AI' formed by Amazon, Facebook, Google, DeepMind, Microsoft and IBM have been looking at the use of potential verification tools to help monitor algorithm performance since 2016, but so far, there is no settled global or cross-sectoral view on how to proceed.[103]

5.1.2 Enhancing AML Investigations

On balance, AML investigator teams have tended to be less of a focus for innovation than TM platforms, largely because of a cost-driven hope amongst MLROs that better technology will lead to a reduction in demand for investigators.[104] But some FIs have also combined platform changes with investment in the development of their investigative cadres, creating global centres of excellence, training academies and career development frameworks. Team cultures have been a particular target, especially in Level 1 and Level 2 teams, where processing high volumes of alerts has tended to encourage investigators to see their work in an industrial light.[105] Responses to this situation have included training and awareness programmes intended to refocus staff on the application of a Risk-Based Approach (RBA), combined with revisions in individual performance assessments to take into account investigation quality as well as throughput of alerts.[106] Interviews further suggest that some FIs have encouraged more joint-working and knowledge-sharing between TM technical and AML investigatory teams, sometimes with short staff attachments and rotations.[107] Along similar lines, one investigatory function in a multinational FI

[101] Author interviews with: (No.8); (No.13); (No.22); (No.29); (No.36); (No.37); (No.47).
[102] Author interviews with: (No.4); (No.14); (No.22); (No.26) regulator panel based in the UK, (10 June 2020); (No.37); (No.38); (No.42).
[103] Institute for Electrical and Electronics Engineers' (IEEE) Standards Association, 'Global Initiative on Ethics of Autonomous and Intelligent Systems,' https://standards.ieee.org/industry-connections/ec/autonomous-systems.html, accessed 13 August 2020; Partnership for AI (PAI) Staff, 'PAI Researchers Co-author Multistakeholder Report on Improving Verifiability in AI Development', (15 April 2020), https://www.partnershiponai.org/pai-researchers-co-author-multistakeholder-report-on-verifying-claims-for-ai-development/, accessed 10 May 2020.
[104] Author interviews with: (No.5); (No.9); (No.10); (No.19) MLRO based in the UK, (3 June 2020); (No.29); (No.38); (No.47).
[105] Author interviews with: (No.3); (No.10); (No.22); (No.29); (No.33); (No.36); (No.40); (No.47); (No.60).
[106] Author interviews with: (No.1); (No.3); (No.10); (No.22); (No.38); (No.47).
[107] Author interviews with: (No.8); (No.13).

was reported to have financially supported the training of some staff in data science, in order to inform their understanding of platform operation.[108]

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. Such tools provide curated views of client networks and connections, and, with the application of advanced techniques such as topological graph theory, have allowed the combination of multiple internal and external data sets for an enriched view of client relationships. Many SNA tools thus increasingly function as integrated intelligence environments, comprising not only transactions and CDD data, but external corporate information procured from vendors, or 'scraped' and translated from the Internet using 'web crawlers' and Natural Language Processing (NLP) techniques.[109]

The effects of investigator-focused reforms are not easy to demonstrate, although interviews indicate that where they have been applied, they can increase investigator morale, and have a direct impact on the quality of work products. One MLRO commented how more joint-working between platform specialists and investigators could lead both "to feel more like trusted professionals on the same team." [110] SNA has also demonstrated its value as a tool for investigation, particularly in Level 3 teams where there is usually more time available to mount a more detailed enquiry. Interviews indicate that network-based platforms can also provide considerable value in complex cases such as sanctions evasion or TBML, where financial crime risks are often revealed less by transactions, and more by unusual relationships.[111]

5.1.3 Risk Monitoring

Further innovations have included the development of additional lines of risk monitoring alongside those pre-existing structures designed to monitor transactions. Interviews suggest that some FIs have moved elements of monitoring into the First Line of Defence in corporate and commercial banking, where it is more feasible for members of frontline staff to track smaller numbers of clients. In these cases, monitoring is supported by separate platforms focused on identifying inconsistent, rather than suspicious activity, with alerts tackled first by relationship managers, before being referred to specialist investigators if alerts cannot be resolved.[112]

More typically, FIs have developed additional risk monitoring capabilities located in internal FIUs or dedicated intelligence and analytics functions. These teams are tasked to use a range of data sources and new technologies – including those mentioned above – to develop proactive assessments of high risk clients, sectors and jurisdictions for a senior internal audience. Although such functions' work can occasionally lead to STRs, it is more likely to be used to shape decisions on client relationships and business strategy.[113] As the former MLRO of a global bank explained, such teams provide a "horizon-scanning role" which can help to mitigate risks and provide "early warning" of potential future problems.[114]

Risk monitoring innovations, typically sat in separate parts of FCC functions from TM, have not had an easily quantifiable impact on FI's monitoring capabilities, but anecdotal reports suggest

[108] Ibid.
[109] Author interview (No.37).
[110] Author interview (No.19).
[111] Author interviews with: (No.7); (No.38).
[112] Author interview (No.55).
[113] Author interviews with: (No.3); (No.8); (No.20); (No.22); (No.55).
[114] Author interview (No.47).

that both frontline and intelligence-style risk monitoring can bring some efficiencies. In the former case, the management of lower level risks in the First Line has allowed smaller teams of specialists in Level 3 AML or FIUs to focus on more complex or concerning investigations, with fewer problematic handoffs.[115] The value of intelligence and analytic products was also stressed by several senior compliance professionals. Such teams have helped to focus FIs more on the operations of networks of 'bad actors' such as organised criminals, kleptocrats and terrorist groups – an example of the previously mentioned 'spear fishing' approach - and have created new understandings of emerging criminal behaviours which have themselves been fed into TM feedback loops.[116] But despite their popularity amongst senior staff, moreover, intelligence and analytics functions can also face difficulties in turning their findings into credible mitigating activity. Compliance and business decision-makers are often puzzled by what to do with material which shows potential financial crime risks based on contextual factors, but which do not provide a 'smoking gun' that can lead to either an STR or an exit.[117]

5.1.4 Next Steps

Ambiguous though the evidence remains about the scale of impact, it appears likely that FIs will continue to follow pre-existing trends in innovation, especially with regard to the use of technology. Although the widespread active deployment of UML for TM appears unlikely in the short term, the prospects for further applications of a variety of other technologies are strong. One currently emerging example is synthetic data, which has been used in recent years to test products and applications as diverse as pharmaceuticals and driverless cars. The data itself can be created in several ways, but a common approach uses 'bots' to mimic known patterns of behaviour to create data sets, such as a body of transactions. Interviews indicate that FIs are beginning to experiment with this type of data to test TM platforms for common typologies and identify theoretical False Negative rates, while one leading regulator is reported to have taken an interest in using such material as way of benchmarking TM platforms' performance.[118]

Most developments, however, are likely to involve further enhancements of pre-existing monitoring and reporting processes with what has been described as 'Augmented Intelligence' (AuI) – the use of automation to make lower-order decisions in real time, as well as select options for human choice on critical matters. Indications of this can be seen in the emerging use of SML to support 'real-time' segmentation and auto-threshold tuning outside of formal optimisation processes. Further steps will also include applying SML not only to risk-rank alerts, but also to make probabilistic assessments on levels of 'suspicion', which investigators would then review; such techniques have already been piloted in one global FI. SNA tools are also evolving into more structured analytic environments, following trends in law enforcement and national security, with data sources automatically prioritised for investigator review.[119] A further AI technique, 'Natural Language Generation' (NLG), also has the capacity to create basic investigative narratives that can be used to provide supporting content for STRs and internal reporting.[120] In most of these instances, algorithms are unlikely to replace humans in the near future – not least because of regulator concerns – but they can provide them with curated options at greater speed.

[115] Author interview (No.55).
[116] Author interviews with: (No.8); (No.19); (No.20); (No.22); (No.40); (No.55).
[117] Author interviews with: (No.8); (No.20); (No.22); (No.55).
[118] Author interviews with: (No.2) RegTech specialist based in UK, (2 June 2020); (No.13).
[119] Author interviews with: (No.7); (No.8); (No.13); (No.31); (No.38).
[120] Author interviews with: (No.13); (No.21).

5.2 FI Innovation Assessment

As with existing innovations, such future developments sound exciting, and might well help push FP rates down further, identify some 'new' illicit activity, and improve the quality of STRs; they should therefore be explored. However, given how limited evidence has proven to be on existing initiatives, a certain amount of caution is necessary before making any assumptions about the extent of improvement that might come from future changes. These new technologies offer FIs the chance to exploit better their own data, but do not 'join the dots' of complex criminal networks across multiple FIs, which is the common *modus operandi* of criminals. Moreover, new technology will not necessarily be workable in all business environments, due to FIs' variations in size, structure and resource constraints. If innovation becomes an option only for larger FIs who can afford it, therefore, there is a serious risk that financial criminal activity could be displaced into the businesses of smaller FIs, 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.

5.3 Regulators and Innovation

FI-led innovation has enjoyed rhetorical support from national regulators in the leading global financial centres such as New York, London, Hong Kong and Singapore. In the US, for example, a joint statement by regulatory agencies in December 2018 noted that "innovations and technologies" could "strengthen BSA/AML compliance approaches, as well as enhance transaction monitoring systems." While remaining 'solution neutral', they also provided assurances that initiatives which revealed pre-existing AML deficiencies would "not necessarily result in supervisory action."[121] The statement further stressed the need for direct engagement with the RegTech industry, and in May 2019, FinCEN started an 'Innovation Hour' programme, giving RegTechs the opportunity to showcase their new technologies within the agency.[122] Similar outreach programmes have developed elsewhere, including the FCA's series of 'TechSprint' workshops, to test new platforms with vendors and FIs. In January 2019, the FCA led the creation of the Global Financial Innovation Network (GFIN) with 38 other financial regulators, including HKMA, MAS and several US federal and state bodies, to shape a similar international programme of global TechSprints.[123] Although the COVID-19 pandemic has slowed this process of direct engagement, leading regulatory bodies remain committed to the innovation agenda, and indeed, it appears that the crisis has in some instances strengthened regulatory support for AML RegTech innovation, as evidenced in FinCEN's April 2020 restatement of the need for FIs "to consider, evaluate, and, where appropriate, responsibly implement innovative approaches" in response to the pandemic.[124]

Such positive attitudes are not universal across the regulatory world, however, and even in the leading jurisdictions, interviews with those working in compliance suggest that progressive policy statements take time to translate into practical experience during examinations. Even where new TM techniques are deployed, moreover, regulators still appear to expect FIs to run dual processes to satisfy the regulatory requirement that 'no STR be left behind,' making regulator-friendly

[121] Board of Governors of the Federal Reserve System (FRS), Federal Deposit Insurance Corporation (FDIC), Financial Crimes Enforcement Network (FinCEN), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), 'Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing' (December 2018).
[122] FinCEN, 'FinCEN announces its Innovation Hours Program', (24 May 2019), https://www.fincen.gov/news/news-releases/fincen-announces-its-innovation-hours-program, accessed 15 October 2020.
[123] For GFIN's membership and scope, see https://www.fca.org.uk/firms/global-financial-innovation-network, accessed 15 October 2020.
[124] FinCEN, 'FinCEN Provides Further Information to Financial Institutions in Response to the Coronavirus Disease (COVID-19) Pandemic', (2 April 2020), https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-provides-further-information-financial, accessed 10 June 2020.

innovation a costly venture. So far, few regulators, however progressive, seem comfortable with the idea of switching any platform off.[125]

Beyond the more supportive jurisdictions, moreover, the majority of regulators wish to maintain a purely 'solution neutral' stance for the time being, while in a few, regulators appear to have been more than a little discouraging. A senior compliance professional from a major European FI opined that many national regulators within the EU, for example, were showing extreme caution with regard to the deployment of machine learning.[126] Why this might be so is not clear, although several interviewees suggested that for the majority of regulators, a lack of in-house technical expertise could be prohibitive when dealing with new technologies.[127] This suggests that if the incremental benefits of FI-led innovation are to spread more widely, leading regulators might also need to play an educators role amongst their peers.

5.4 Regulators and TM Management

Leading global regulators have not only been responding to technological innovation, but also to the wider issue of 'what good looks like' in TM management. MAS, HKMA and other institutions such as De Nederlandsche Bank (DNB), the Netherlands' national bank, have issued detailed guidance on TM frameworks in recent years, setting out principles-based approaches to key issues in implementation and management.[128] While continuing to emphasise the need for an RBA, these guidance documents provide a comprehensive view of the issues to be addressed at different stages of the TM lifecycle, with anonymised examples of good and bad practice from regulatory examinations interwoven throughout.

In contrast, another leading regulator, New York State's Department for Financial Services (NYDFS), has taken a more prescriptive stance. In its Rule 504 on TM and Sanctions Screening, issued in January 2017, the Department requires FIs to follow precise model validation protocols, and to submit detailed supporting documentation, along with a board-level attestation of compliance, on an annual basis. The Rule also mandates FIs to monitor not only for money laundering and terrorist financing, but "Specified Unlawful Activities (SUA)" such as predicate money laundering offences and tax evasion.[129]

Given the character of the problems facing TM, such regulatory initiatives are unlikely to tackle the underlying problems – identifying suspicious activity in limited data sets – but they do offer the prospect of improving the manner in which TM frameworks are run, potentially reducing friction between regulators and FIs. Of the two strategies outlined, a principles-based approach appears less likely to push FIs into undertaking activities that are not appropriate to their risk context. But it is far from certain that principles-based guidance, applied as 'for information only', would have a wide sectoral impact, especially amongst mid- and lower tier FIs who enjoy less regulatory contact than those in the top tier. Considered from this perspective, therefore, the mandatory underpinnings of Rule 504 might have some value. As a senior US compliance professional commented, although the prescriptive aspects of the Rule are "onerous," the concept of attestation "is not a bad thing in principle. It concentrates minds."[130] This suggests

[125] Author interviews with: (No.5); (No.9); (No.14); (No.27); (No.29); (No.42); (No.47); (No.58).
[126] Author interview (30).
[127] Author interviews with: (No.4); (No.7); (No.8); (No.9); (No.13); (No.20); (No.21); (No.30); (No.34); (No.37); (No.47).
[128] De Nederlandsche Bank (DNB), 'Post-event Transaction Monitoring Process for Banks: Guidance', (August 2017); Hong Kong Monetary Authority (HKMA), 'Guidance Paper: Transaction Screening, Transaction Monitoring and Suspicious Transaction Reporting', (Revised May 2018); Monetary Authority of Singapore (MAS), 'Guidance for Effective AML/CFT Transaction Monitoring Controls', (September 2018).
[129] New York Department of Financial Services (NYDFS), 'Superintendent's Regulations: Part 504 – Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications', (January 2017).
[130] Author Interview (No. 15).

that a hybrid approach might be one way forward, with FIs attesting to the application of the principles-based guidance. This would offer a prospect of both improving the sectoral penetration of good practice, without compromising the RBA.

5.5 Financial Intelligence Sharing Partnerships (FISPs)

LEAs and FIUs have largely not been involved in internal FI innovations or regulatory initiatives, but they have played an important parallel role in the development of Financial Intelligence Sharing Partnerships (FISPs) with FIs. 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.[131] 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 STR filings might be of value to an LEA or disseminate strategic intelligence reports on criminal behaviours and typologies. In a smaller number, such as Australia's Fintel Alliance, there is also direct joint-working between public and private sector investigators, and there have been further *ad hoc* examples of this during the pandemic, as both have worked together against health related frauds.[132] Alongside institutional relationships, several jurisdictions also have legal safe harbours for partial private-private sharing, such as Section 314 (b) of the PATRIOT Act 2001 in the US, and the UK Criminal Finances Act (CFA) of 2017.[133]

These 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.[134] 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. The next step for many FISPs therefore is likely to be the widening of pre-suspicion intelligence sharing within the private sector, to allow details of investigations to be shared between FIs' AML investigators prior to engaging the public sector. Such changes could be either supported by alterations to data sharing laws – which are increasingly stringent in preventing the sharing of clients' personal information – or the deployment of encryption techniques, such as Privacy Enhancing Technologies (PET), which can be used across multiple data sets to undertake sharing and analysis without revealing underlying personal data.[135] This presents the possibility of FIs creating more integrated intelligence pictures for LEAs in joint STRs.

5.6 FISPs and TM

The focus of FISPs so far has thus been on 'downstream' activities of AML investigation and reporting, and less on the 'upstream' matter of what kind of alerts are produced. As a result,

---

[131] Maxwell, Nick J., 'Five Years of Growth in Public–Private Financial Information-Sharing Partnerships to Tackle Crime', *RUSI Future of Financial Intelligence Sharing (FFIS) Report*, (July 2020); Maxwell, Nick J., and David Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', *RUSI Occasional Paper* (October 2017).

[132] Author interviews with: (No 28); (No.40); see also Chaderton, Paula, Simon Norton, 'Public-Private Partnerships to Disrupt Financial Crime: An Exploratory Study of Australia's FINTEL Alliance', *SWIFT Institute Working Paper, 2017-003*, (May 2019), https://swiftinstitute.org/research/public-private-partnerships-to-disrupt-financial-crime-an-exploratory-study-of-australias-fintel-alliance/, accessed 23 February 2021.

[133] FinCEN, 'Section 314(b) Fact Sheet', (November 2016); UK Home Office, 'Circular: Criminal Finances Act 2017 Money Laundering: Sharing of Information within the Regulated Sector Sections 339ZB-339ZG'(1 February 2018).

[134] Maxwell, Nick J., 'Five Years of Growth in Public–Private Financial Information-Sharing Partnerships to Tackle Crime', *RUSI/FFIS,* (July 2020), p.18.

[135] Maxwell, Nick J., 'Case studies of the use of privacy preserving analysis to tackle financial crime,' *RUSI Future of Financial Intelligence Sharing (FFIS) Innovation and Discussion Paper,* (June 2020), pp.9-10.

partnerships have largely failed to improve the quality and relevance of TM alerts and the bulk of proactive STRs that arise from them.[136] The dissemination of LEA insights into criminal typologies through FISPs has been a step towards this, but the volume of sharing varies between jurisdictions, is often episodic, and is more typically framed around the needs of AML investigators than TM platform managers.[137] A scaling up of operationally demonstrable and risk-relevant typology sharing centred around LEA priorities could potentially help, therefore, but would have to be framed around the needs of all relevant stakeholders to have greater impact. In the first instance, this implies more direct engagement by technology specialists in FISPs, alongside investigators, to ensure that the information being shared is usable in platform detection scenarios. It further suggests the need for LEAs to use FISPs to provide clearer guidance on strategic reporting priorities, to avoid the creation of multiple new streams of unproductive reporting. The value of different detection scenarios might vary over time, or between different types of FIs, and FISPs could play a role in guiding these assessments. Such an approach might prove controversial in light of current regulatory philosophies that stress the need for comprehensive risk coverage in TM platforms. However, it would at the very least provide a demonstrable opportunity to align FI and LEA priorities, reduce wastage in the current monitoring and reporting framework, and potentially provide a simpler set of metrics with which FIs – and regulators – could assess whether TM 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.

5.7 Conclusion

No package of reform will make the current monitoring framework a perfect mechanism for detecting and delivering financial intelligence, and expectations of such are unrealistic. However, it is credible to believe that it might more accurately detect real underlying risks in transactions, reducing False Positives and False Negatives.

Taken as a whole, the innovations discussed in this chapter are likely to deliver some reductions in waste in the pre-existing AML ecosystem. Although evidence of impact is limited at present, it is reasonable to suppose that enhancing platform performance and improving training and morale, along with increased regulator and LEA support and guidance, will help FIs to identify less complex forms of illicit activity in their data with more precision, lowering FPs, improving STR conversion rates and delivering higher proportions of relevant reporting to LEAs. However, none of the initiatives – even most FISPs as currently conceived – will be able to overcome the institutional data barrier that makes it impossible for individual FIs to see the wider strategic network of criminality in the financial system. More radical extensions of the concept of information sharing – private-private and public-private – will be needed to ensure that AML/CFT structures can respond to the fluid nature of financial crime and refocus on its core purpose: creating actionable intelligence for LEAs.

[136] Author interviews with: (No.1); (No.4); (No.10); (No.19); (No.25); (No.28); (No.36); (No.38); (No.47).
[137] Author interviews with: (No.20); (No.29).

6. Systemic Solutions

If monitoring is to create a more accurate understanding of financial crime, the fragmentation of the current approach thus 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 – some version of systemic monitoring – has thus gained some support over the last five years, encouraged by the development of KYC utilities and FISPs. So far, prototypical TM initiatives have emerged at national levels in only a handful of jurisdictions, most notably 'Transaction Monitoring Netherlands' (TMNL), a TM utility created in the private sector but with significant official support, although data privacy hurdles still need to be cleared and reduced by authorities.[138] Utilities are not the only potential systemic alternative, however, and experiments with monitoring across payments architectures or under the auspices of public sector agencies, have also been tried or are being discussed.

As one might expect, early evidence from these projects suggests that systemic monitoring can provide a clearer view of complex criminal behaviours and relationships – as long as sufficient data and market coverage can be attained. More difficult challenges come from the many practical barriers that restrain multiple stakeholder initiatives, especially those led by the private sector. Technical and data law challenges are similar to those for FISPs, and there are added legal dimensions around competition and liability laws. Though not insurmountable, they demand long-term commitment to resolve.

Although it seems unlikely that one systemic solution will necessarily suit all jurisdictions, the fewest legal issues would probably come through a public sector-led approach, which would also have the potential to be more streamlined than the current model. Of course, public sector-led monitoring is not without its own challenges, as it would require a significant rebalancing of responsibility in the AML ecosystem. Nonetheless, such questions of capability and resource could potentially be addressed, at least initially, through joint public-private resourcing.

6.1 The Emergence of Utilities

Industry interest in systemic perspectives developed initially in the KYC space, around the time of the last major revision of FATF's 40 Recommendations in 2013. With the expansion of private sector obligations, and the ongoing problems that FIs faced in meeting them, several major financial information providers, including the Society for Worldwide Interbank Financial Telecommunications (SWIFT), began developing centralised KYC utility services, as a way to provide FIs with a more complete view of clients and potential clients.[139] This 'shared-service' approach generated further interest amongst regulators and FIs, leading to a number of initiatives at national and regional levels. Indian authorities launched their own KYC utility in 2016, and authorities in Singapore and Hong Kong, amongst others, have explored the potential of such schemes. A cross-border utility, MANSA, was launched by several African banks in July 2018, and a similar bank-led scheme in the Nordic countries remains in development.[140]

---

[138] Couvee, Koos, 'Dutch Banks Forge Ahead with Joint Transaction Monitoring' *ACAMS,* (5 August 2020), https://www.moneylaundering.com/news/dutch-banks-forge-ahead-with-joint-transaction-monitoring/, accessed 5 August 2020.

[139] Twomey, Niall, 'KYC Utilities: The Second Coming, Learning from Past Failures', *Finextra*, (11February 2020), https://www.finextra.com/blogposting/18446/kyc-utilities-the-second-coming-learning-from-past-failures, accessed 12 March 2020.

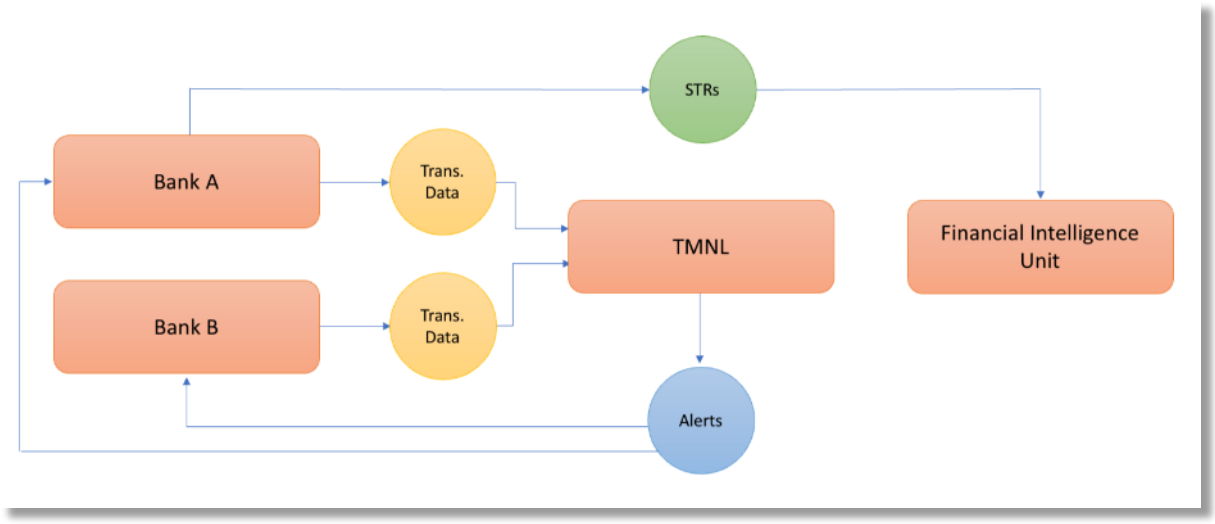
[140] IIF & Deloitte, 'The Global Framework for Fighting Financial Crime: Enhancing Effectiveness & Improving Outcomes', (2019), p.22; Fintech Futures, 'Regional KYC utilities: Genesis of global collaboration on shared compliance platforms', (17 November 2019), https://www.fintechfutures.com/2019/11/regional-kyc-utilities-genesis-of-global-collaboration-on-shared-compliance-platforms/, accessed 20 June 2020.

6.2 TM Utilities

The prevalent focus on KYC in utility projects has been the natural result of the centrality of the CDD obligation in AML international standards, as well as a political environment which has emphasised the importance of corporate transparency since the Great Financial Crisis of 2007-08. The collation of static client data has also appeared to be technically easier to achieve than the monitoring of ongoing activity, and there has been a widespread assumption that because many TM platforms now feature client segmentation based on risk groupings, a TM utility would presuppose the need for a KYC utility as a source of such segmentation data.[141]

Nonetheless, discussions around possible TM utilities have developed in a handful of jurisdictions in the last two to three years. 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 TM utility supported by the private sector. Of the two, TMNL has made by far 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.[142]

FIGURE 7 – Basic TMNL Outline[143]



The diagram above gives a basic model of how TMNL is expected to work, with the participating banks sharing their transactions data with the third-party utility, where a shared platform will monitor for unusual activity – the Netherlands' legal standard – and then send alerts back to the individual banks for further investigation and then potential onward reporting to the FIU.

The utility's platform is a 'new build', and not based on the legacy platforms of its participants', with institutions' data pooled by using PET to protect privacy and security. Initially, the platform will use a rules-based approach, with detection scenarios created by discussions between the

[141] Author interviews with: (No.9); (No.32); (No.43) compliance consultant based in Sweden, (24 June 2020).
[142] Author interviews with: (No.11); (No.12); (No.13); (No.41), compliance consultant panel based in the Netherlands, (23 June 2020); (No.44) compliance consultant based in the Netherlands, (16 July 2020); (No.46) compliance consultant panel based in the UK, (14 May 2020); (No.54) senior compliance leader based in the Netherlands, (19 May 2020); Maxwell, Nick J., 'Case studies of the use of privacy preserving analysis to tackle financial crime,' *RUSI/FFIS,* (June 2020), pp.32-33; (No.41).
[143] Author diagram based on information collated in footnote 139.

individual FIs, with SML and other more advanced techniques potentially introduced over time. The initial focus will be on mid-tier corporates and small businesses, a sector in which the five banks have 80% coverage of relevant transactions in the country. Nonetheless, the eventual ambition of TMNL is to offer a solution that covers all client types. It is expected that the participating banks will continue to run their own TM platforms while the project seeks to demonstrate value.[144] This parallel work comes at a significant cost to the private sector and is a demonstration of their commitment to fight financial crime together for society.

6.3 Utility Prospects

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 FP 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.[145] Despite the concerns of some that a TM utility would not be feasible without a KYC utility in place first, reports from TMNL suggest otherwise, as unusual activities stand out more starkly in large data sets; as an individual familiar with the project commented, "the quantity of data involved has created a qualitative difference of its own."[146]

A certain amount of caution is required, however, before assuming that TM utilities are a universal solution to the current problems with monitoring. TMNL, for one, remains at an early stage, and although the atmospherics 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 an FI level. Theory suggests that they *should* be better, but this has yet to be conclusively demonstrated with publicly available information. It is also uncertain whether better alerts will lead to more valuable and relevant STRs, and consequently to more LEA action and recovery, especially if individual FIs continue to mount many separate AML investigations. There is a very obvious danger of ongoing duplication of effort and unnecessary reporting as a result, which would suggest the need for pre-suspicion sharing protocols and cross-institutional investigative structures to ensure that the benefits of 'upstream' sharing were not stymied 'downstream.'

Set against these potential but as yet unproven benefits, privately-led TM utilities also face many of the same challenges of deliverability as their KYC counterparts. Data is the primary issue, and as interviews with those involved in other utility projects suggest, breadth of coverage is vital. In the case of TMNL, the five participants dominate their national financial system, but in other instances where a less comprehensive body of data has been available, the benefits of consolidation are reported to be less impressive.[147] Data quality, consistency and access will also affect performance, and in jurisdictions where TM 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.[148]

The experience of both KYC utilities and TMNL so far further suggests that private-sector led utilities will face significant legal challenges. Some of these are familiar to those involved in FISPs,

[144] Author interviews with: (No.41); (No.44); (No.54).
[145] Author interviews with: (No.41); (No.44).
[146] Author interview (No.44).
[147] Author interviews with: (No.12); (No.46); (No.50).
[148] Author interviews with: (No.13); (No.14); (No.29).

such as the difficulties around sharing of client data between private institutions, which 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.[149] More than that, however, 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 TM utility is not yet wholly apparent.[150]

TMNL's progress so far suggests that some of these difficulties can be overcome with a "whatever it takes" attitude towards costs and delivery. Nonetheless, the project also depends on strong governmental support and action, and TMNL has already had to look to the government of the Netherlands' to change relevant laws to allow outsourcing and transaction data sharing.[151] This kind of sustained political support cannot be taken for granted, or assured in all jurisdictions, suggesting that TMNL will need to demonstrate clearly improved outcomes if it is to be emulated elsewhere.

6.4 Payments Monitoring

Although TM utilities are reliant on the internal transactions data of FIs, 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. Individual jurisdictions are increasingly seeking to rationalise and speed up these systems, and in the Eurozone, the European Central Bank (ECB) has sought to encourage a more standardised approach, creating the Single European Payments Area (SEPA) a decade ago. 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.[152]

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. Based on an original exercise using two years of FPS data, MITS created a strategic map of money mule networks – those used as proxies by organised crime groups to deposit and transfer illicit funds – and developed a platform using live data that could alert subscribing banks' fraud teams in real-time of suspect payments, allowing them to block those payments if necessary. In October

[149] Author interview (No.43); Hillenius, Giljs, 'Swedish Procurement Study: Web-based Office Tools Not GDPR Compliant', *Open Source Observatory*, (26 February 2019), https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/security-and-compliance, accessed 12 October 2020.
[150] Author interviews with: (No.41); (No.44); (No.43).
[151] Ibid.
[152] See https://www.swift.com/our-solutions/compliance-and-shared-services/business-intelligence/swift-scope, accessed 10 February 2021.

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.[153]

6.5 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.[154] If applied in an integrated way across a larger number of payment systems, a MITS-style tool could help FIs 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 FIs. Payments systems typically use account numbers as identifiers, allowing platforms to track suspect behaviour without the need to have access to the personal data behind the numbers.

Such a system could also dovetail with the use of 'blockchain', or Distributed Ledger Technology (DLT), to execute and record financial movements between FIs. Blockchain experts suggest that tokenised versions of fiat currencies could be transferred via algorithmic 'smart contracts' which would be validated by FIs – or 'nodes' – in the dispersed network.[155] Such contracts would contain automated analysis to identify indicators of potential risk, or the involvement of suspect counterparties, creating alerts for participating FIs. The record of the alert would then also become part of the shared history of the network.

However, whether managed through blockchain or traditional fiat systems, payments monitoring would not produce as potentially 'rich' a data picture as a platform which also had access to client information. It would still also face at least some of the same practical challenges as a TM utility. Adequacy of coverage would depend on levels of participation from the FIs who make up the network, and alerts would still need to be delivered to individual institutions for investigation and reporting. Moreover – and most damaging to the prospects of imminent deployment – is a basic problem of incentives. Payments networks do not have AML reporting and monitoring responsibilities, and it is notable that MITS has developed as a subscriber service. Until the commercial potential of selling such services grows more widely, therefore, 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.

6.6 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.[156] There are no working examples of such

[153] Clelland, Victoria, 'Enhancing Resilience In Payments', *The Bank of England speech at PayExpo 2019* (8 October 2019), p.6, https://www.bankofengland.co.uk/-/media/boe/files/speech/2019/enhancing-resilience-in-payments-speech-by-victoria-cleland.pdf, accessed 1 October 2020.
[154] Emerging Payments Association (EPA), 'Facing up to Financial Crime: Analysis of payments-related financial crime and how to minimise its impact on the UK', (2018), p.24.
[155] DeCosta, Floyd, 'Blockchain for AML: Harnessing Blockchain Technology to Detect and Prevent Money Laundering', *The International Banker,* (10 November 2017), https://internationalbanker.com/technology/blockchain-aml-harnessing-blockchain-technology-detect-prevent-money-laundering/, accessed 12 April 2020.
[156] Author interviews with: (No.8); (No.22); (No.19).

an approach at present, 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 FI's transaction databases with PET, and then applying machine learning analytics to the encrypted data. Under the current plans, suspect transactions will be delivered to the relevant FIs, who will then be expected to provide relevant client details to AUSTRAC, the Australian FIU, for further dissemination and investigation.[157]

At the time of writing, the Alerting Project remains in development, and there is no empirical evidence on which to judge the scheme. However, in theory at least, it does appear to offer the advantage of other systemic approaches – a network-wide perspective covering all FIs' data – with fewer additional constraints. Technological implementation would remain a challenge, but many of the problems that hamper TM utilities with regard to data sharing, commercial law, liability and regulation would be less likely to occur with direct public sector leadership. There would also be potential further operational benefits; the monitoring agency would be able to take a 'risk-focused' approach driven by investigative and intelligence collection priorities, and FIs would only be required to provide encrypted access to their data and deliver client related material to LEAs upon request. From FIs' perspective, the monitoring burden would be reduced, or possibly even eliminated.

Radical though such an approach might sound, its basic assumption – that the private sector provide the public sector with wide-raging access to specific types of financial material – has precedents in some countries' AML laws. In the US, Australia, Canada and Mexico for example, FIs are already mandated to disclose data to FIUs on certain types of activity, such as bulk cash transactions, cross-border Electronic Funds Transfers (EFTs), large value transactions and foreign currency transactions, which the respective FIUs then analyse.[158]

Nonetheless, a public sector-led model would undoubtedly require significant political will and investment to succeed. Although some LEAs might be able to take up a monitoring responsibility quickly, most would not, and the vast majority of FIUs are often not much more than administrative clearing houses for STRs at present. Such a shift in responsibility would thus raise a basic question of 'who will pay' for the change. Governments might be wary of looking to taxpayers to support the cost of a requirement previously undertaken by FIs, and it might therefore be necessary for the financial services sector to provide resources and support to enable such a shift, at least initially. One MLRO of an international bank suggested this might be feasible, however, as a "grand bargain," along lines similar to the UK government's prospective 'Economic Crime Levy'. FIs would support the necessary investments in the public sector financially, and through ongoing support in expanded FISPs. However, this would only be an attractive option to FIs if it were a genuine 'quid pro quo', which allowed them to reduce their monitoring efforts and the associated costs over time.[159]

6.7 Conclusion

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

[157] Maxwell, Nick J., 'Case studies of the use of privacy preserving analysis to tackle financial crime,' *RUSI Future of Financial Intelligence Sharing (FFIS) Innovation and Discussion Paper,* (June 2020), pp.34-35.
[158] Poncy, Chip, and Juan C. Zarate, 'Designing a New Anti-Money Laundering (AML) System', *Center on Sanctions and Illicit Finance Research Memo* (September 2016), p.10.
[159] Author interview (No.19).

realistic way, given technical and legal constraints. All the examples have their own varied problems of implementation, which are likely to take time, trust and willpower to overcome. Some issues of process – such as the question of who handles the alerts – are likely to become more important as the projects proceed, and potential friction points and bottlenecks become more obvious. From the perspective of this study, a public sector-led approach appears the least problematic way forward, despite its own frictions. At root, it is a question about identifying the best way to fight financial crime, rather than focusing on protecting the working practices of a framework that has so far failed to deliver.

Conclusion and Recommendations

The problems with the current approach to AML monitoring and reporting are unambiguous. Across the financial services sector, TM frameworks produce streams of alerts which are mostly discarded by FIs, leading to STRs which go mostly unused by LEAs. All this comes at significant financial cost too, and with the additional risk of regulatory censure for FIs. Although it is difficult to quantify this judgement, the current approach appears to entail a great amount of effort, for a disproportionately small amount of reward.

This situation has no single explanation or cause. Contextual problems of technology, resource and internal organisational frictions can affect performance, as too can poor decision-making within FIs. But at its core, TM, as conducted across most of the industry, is focused on an inherently difficult task: to identify the indicators of suspicious activity, within the confined data set of an individual FI'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, an FI 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. As a most basic reform, therefore, FATF and its member governments need to look again at the expectations of individual FIs in this regard.

Recommendation 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, FIs should at most 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.

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

A. Improving the Current System

Such a review is not likely to take place quickly, of course, and in the meantime, the industry will continue to operate on its current assumptions – identifying and reporting suspicion at an institutional level – while seeking to do this with lower levels of False Positives, cost, reduced regulatory challenge and improved effectiveness. As reviewed earlier, FIs are undertaking a range of initiatives at varying stages of maturity to support these goals, including:

- High tempo and frequent platform optimisation.
- Integration of wider FCC feedback into TM optimisation processes.
- Use of automation and machine learning to optimise platforms and prioritise alerts.
- Development of a 'risk-focused' culture in AML investigations.
- Use of network analysis in advanced and specialist investigations.
- Deployment of additional layers of *risk* monitoring in the First and Second Lines.
- Use of synthetic data in testing for False Negative rates.

From the perspective of efficiency and the smoother working of the current AML ecosystem, these efforts should of course be encouraged, not only because they will potentially reduce the burden on FIs, but also reduce the amount of unused (or unusable) financial intelligence passing from the private to the public sectors. However, expecting such initiatives to diffuse naturally throughout the sector and to be uniformly applied is unrealistic. This kind of reform agenda is now common amongst top tier FIs, but less so at lower levels. To ensure that the knowledge of good practice is more widely disseminated and applied across the industry therefore, regulators will need to use mechanisms available to them.

Nonetheless, FIs should avoid the pursuit of innovation for innovation's sake, and a key aspect of evolving regulator guidance will need to be assessments of the costs and benefits of certain types of technology (if not individual platforms) as they develop. This will include maintaining a 'weather eye' on the development of more forward-looking technologies such as UML or levels of platform automation, as well as providing guidance on the contextual requirements of different types of innovation.

Recommendation 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.

Recommendation 3: National regulators, following examples such as Singapore, Hong Kong and the Netherlands, should issue guidance on reasonable TM model management and governance, providing good practice examples for all relevant activities. Such guidance should be principles-based and allow flexibility for context and an RBA.

Recommendation 4: National regulators should consider the value of FIs annually attesting to the completion of key TM platform performance and governance tasks.

It is imperative that regulators take up these challenges, as they will be essential partners for FIs if technological innovation is to bear fruit. Although the point is relevant to more than just TM, it should go without saying that national regulators *should* also be resourced and equipped to deal will technological issues themselves, rather than relying on FIs to take the lead. If national regulators do not pick up the baton, they should be encouraged to do so by FATF, which itself should look to governments to take appropriate action. Industry bodies such as the Wolfsberg Group might also look to issue their own industry standards and good practice guidelines, but is not reasonable to look to the private sector to lead alone on these issues. Efforts have to be collaborative.

In parallel to these internal FI reforms and regulatory efforts, public-private FISPs have proved a useful way to focus FI 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, as would their development at an international level in the longer term, given the transational character of financial crime. Of the options available within the bounds of the current AML ecosystem, FISPs are the best channel through which not only investigators, but TM platform specialists and regulators, 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.

Recommendation 5: FISPs should develop basic feedback mechanisms that identify for FIs 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 LEAs with timely feedback on individual STRs as well as priority typologies.

Recommendation 6: FISPs should develop working groups for the discussion of how priority typologies can be translated into TM detection scenarios. This should involve the active involvement of TM specialists from both sectors.

Recommendation 7: FISP should explore their capacity to act as 'tasking channels' for directing the collection of thematically significant intelligence by TM in specific investigative areas selected by LEAs, to improve the relevance of proactive STRs.

Recommendation 8: Alongside examinations of technical compliance and implementation effectiveness, national regulators should include an FI's delivery against FISP defined reporting priorities as an assessment of outcome effectiveness, as suggested by The Wolfsberg Group in December 2019.
(*https://www.wolfsberg-principles.com/articles/wolfsberg-group-statement-effectiveness-2019*)

To follow this path – aligning some aspects of TM and AML investigations more closely with LEA priorities – would require the involvement and explicit support of regulators, because the prioritisation of detection scenarios is likely to interfere with current regulatory expectations about breadth of risk coverage. To take this into account, the scope of regulatory TM examinations will need to change.

B. Limits to Reform

Taken together as a 'reform package', recommendations 1 to 8 are likely to further improve the performance of current TM frameworks further, reducing numbers of False Positive alerts and providing further focus for FI reporting, while simultaneously reducing costs and grounds for friction between FIs and regulators. Nonetheless, the improvements that will accrue are likely to remain incremental. New technologies and wider partnerships will provide more precision in detecting the 'known unknowns' in transactions and wider datasets, but however proficient platforms and investigators become, there will still be significant problems with looking for complex crimes in a single FI's data. Many blind spots will remain hidden in the institutional gaps between FIs, even with the help of FISPs.

Nor is this reform package likely to be universally translatable across every FI or jurisdiction. Increasing the tempo of platform optimisation will be easier in a mid-tier FI than a global multinational, while heavy investment in training programmes, staff retention or experiments with structural changes or technological innovation will be considerably easier for top tier institutions. In the latter instances, deeper pockets will afford greater advantages, increasing the risk of a 'monitoring gap' between leading FIs and their many competitors and a displacement of

illicit activity from large to smaller institutions. Illicit activity would not be reduced overall, so much as passed around the industry.

C. Systemic Options

Systemic options could more significantly reduce opportunities for criminal networks to hide in the coverage gaps that currently exist between FIs and, if suitably broad-based, could mitigate the risk of illicit activity displacing between institutions at different levels of monitoring maturity. Early anecdotal results of reduced FPs and the detection of previously unknown illicit activity from TMNL are broadly positive, but publicly available evidence remains thin. In theory, systemic monitoring should be more effective than the current institution-by-institution model, but this has not yet been demonstrated in empirical terms.

This current absence of evidence on outcomes and impact is likely to be a disincentive to some governments and FI consortia, especially given the significant implementation challenges and initial costs involved in such projects. As KYC utilities have already demonstrated, it is a long road from idea to delivery. Any systemic option is likely to involve many stakeholders and complex questions of cost, resource and project management, with private-led projects facing particularly acute challenges around data privacy, competition law, liability and accountability and public sector-led alternatives questions of political will and financial responsibility. As the progress of TMNL suggests, such practical difficulties are not necessarily beyond solution, but they are numerous, far from all resolved, and are likely to generate persistent frictions in delivery which will vary, depending on the political, economic and legal realities of each jurisdiction.

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 FI would be obligated to provide access to their data. FIs would still need to interact with law enforcement to provide client material on request, but FI 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 or with respect to certain types of financial crime risk, especially if the level of state investment needed to make such a public sector approach possible would be difficult to secure and no public-private funding solution could be established. These are issues which each jurisdiction should explore in their own right, and should be encouraged to do so.

Recommendation 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.

Recommendation 10: FATF should encourage the progress of systemic solutions in individual jurisdictions, and develop risk-based guidance to support individual jurisdictional initiatives.

Glossary

Glossary			
AML	Anti-money laundering	MSB	Money Service Bureau
CDD	Customer Due Diligence	NBFI	Non-Banking Financial Institution
CFT	Counter Terrorist Financing	NLG	Natural Language Generation
DNFBPs	Designated Non Financial Businesses and Professions	NLP	Natural Language Processing
EDD	Enhanced Due Diligence	PEP	Politically Exposed Persons
EWRA	Enterprise Wide Risk Assessment	PET	Privacy Enhancing Technology
FATF	Financial Action Task Force	PoC	Proceeds of Crime
FCC	Financial Crime Compliance	RBA	Risk-Based Approach
FISP	Financial Intelligence Sharing Partnerships	RPA	Robotic Process Automation
FIU	Financial Intelligence Unit	SAR	Suspicious Activity Report
JMLIT	Joint Money Laundering Task Force	SML	Supervised Machine Learning
KYC	Know Your Customer	SNA	Social Network Analysis
LEA	Law Enforcement Agency	STR	Suspicious Transaction Report
MER	Mutual Evaluation Report	TMNL	Transaction Monitoring Netherlands
MLAT	Mutual Legal Assistance Treaties	UML	Unsupervised Machine Learning
MLRO	Money Laundering Reporting Officer	VASP	Virtual Assets Service Provider

Bibliography

AML/CFT Industry Partnership (ACIP), 'Industry Perspectives – Adopting Data Analytics Methods for AML/CFT', (November 2018).

Adams, Heather, Saad Choudri, Philippe Guiral, Samantha Regan, 'Evolving AML Journey: Leveraging Machine Learning within Anti-Money Laundering Transaction Monitoring', *Accenture Consulting,* (2017).

Adams, Heather, Philippe Guiral, Nirmal Khachane, Bharat Mittal, 'Intelligent Automation and Advanced Analytics to Power Financial Crime Compliance', *Accenture Consulting*, (2019).

Association of Intelligent Information Management (AIIM), 'What is Robotic Process Automation?', https://www.aiim.org/What-is-Robotic-Process-Automation, accessed 1 October 2020.

Atkinson, John, Carol Beaumier, Luis Canelon, Carl Hatfield, Bernadine Reese, Chetan Shah, 'Views on AML Technology. Volume I: From System Selection to Effective', *Protiviti*, (November 2013).

—— 'Views on AML Technology. Volume II: Validation, Selection, Metrics and More', *Protiviti*, (November 2014).

Babuta, Alexander, Ardi Janjeva, Marion Oswald, 'Artificial Intelligence and UK National Security Policy Considerations', *RUSI Occasional Paper,* (April 2020).

Bailey, Natalia, 'IIF Machine Learning Recommendations for Policymakers', (September 2019).

Bayley, Nick, '2020 AML Fine Values Already Surpass 2019 as Firms are Repeatedly Sanctioned for the Same Failings' *Duff and Phelps*, (10 August 2020), https://www.duffandphelps.com/about-us/news/duff-phelps-global-enforcement-review-2020-launched, accessed 10 September 2020.

Besbes, Nesrine, Rafael Gomes, Samantha Regan, Ben Shorten, '2018 Compliance Risk Survey: Comply and Demand', *Accenture Consulting,* (2018).

Bevan, Oliver, Piotr Kaminski, Ida Kristensen, Thomas Poppensieker, and Azra Pravdic, 'Compliance at an Inflection Point,' *McKinsey and Company*, (January 2019).

Board of Governors of the Federal Reserve System (FRS), Federal Deposit Insurance Corporation (FDIC), Financial Crimes Enforcement Network (FinCEN), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), 'Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing', (December 2018).

Branisteanu, John, David DeLeon, Philippe Guiral, Samantha Regan, 'Evolving AML Journey: Operational Transformation of Anti-Money Laundering Through Robotic Process Automation', *Accenture Consulting,* (2017).

Canelon, Luis, Andrew Clinton, Bernadine Reese, 'Views on AML Transaction Monitoring Systems: From System Selection to Effective Governance', *Protiviti,* (November 2013).

Chong, Alberto, and Florencio López-de-Silanes, 'Money Laundering and its Regulations', *Working Paper, No. 590, Inter-American Development Bank (IDB)*, (February 2007).

Clark, Robert M., *Intelligence Analysis: A Target-Centric Approach*, 6th Edition, (Sage: London, 2020).

Clelland, Victoria, 'Enhancing Resilience In Payments', *The Bank of England speech at PayExpo 2019* (8 October 2019), p.6, https://www.bankofengland.co.uk/-/media/boe/files/speech/2019/enhancing-resilience-in-payments-speech-by-victoria-cleland.pdf, accessed 1 October 2020.

Couvee, Koos, 'Dutch Banks Forge Ahead with Joint Transaction Monitoring', *ACAMS* (5 August 2020), https://www.moneylaundering.com/news/dutch-banks-forge-ahead-with-joint-transaction-monitoring/, accessed 5 August 2020.

Craig, Patrick, Aaron Gross, Matthew Reed, Rafael Pontes (EY), 'Advanced Risks, Advanced Opportunities?', *inCOMPLIANCE* Issue 29 (May 2017), pp.34-36.

Craig, Patrick, Mark Gregory, Tom Salmond (EY), 'Financial Crime 2.0', *inCOMPLIANCE* Issue 33 (March 2018), pp.25-28

Craig, Patrick, Jodie Forbes, Eamon Howard, Becky Marvell, Matt Reed, 'Anti-Money Laundering (AML) Transaction Monitoring: 2018 EMEIA Survey Report', *EY*, (October 2018).

Davies, Howard, and Maria Zhivitskaya, 'Three Lines of Defence: A Robust Organising Framework, or Just Lines in the Sand?', *Global Policy,* Volume 9, Supplement 1, (June 2018), pp.34-42.

Davison, Nick, Damian Kalinowski, Richard Major, 'Towards Better Transaction Monitoring', *PwC*, (March 2019).

DeBrusk, Chris, Allen Meyer, Adrian Murphy, Elena Belov, 'Embarking on a Journey from "Surveillance" to "Detection"', *Oliver Wyman* (2017).

DeCosta, Floyd, 'Blockchain for AML: Harnessing Blockchain Technology to Detect and Prevent Money Laundering', *The International Banker,* (10 November 2017), https://internationalbanker.com/technology/blockchain-aml-harnessing-blockchain-technology-detect-prevent-money-laundering/, accessed 12 April 2020.

De Jong, Karin, Hilko van Rooijen, 'Advanced analytics in Transaction Monitoring', *Deloitte* (2018).

De Nederlandsche Bank (DNB), 'Post-event Transaction Monitoring Process for Banks: Guidance', (August 2017).

Desai, Devan R., and Joshua A. Kroll, 'Trust But Verify: A Guide to Algorithms and the Law', *Harvard Journal of Law & Technology,* (Volume 31, No.1, Fall 2017).

Domingos, Pedro, *The Master Algorithm,* (London: Penguin Books, 2015).

Emerging Payments Association (EPA), 'Facing up to Financial Crime: Analysis of payments-related financial crime and how to minimise its impact on the UK', (2018).

European Commission, 'Preventing Money laundering and Terrorist Financing across the EU. How does it work in practice?' https://ec.europa.eu/info/sites/info/files/diagram_aml_2018.07_ok.pdf, accessed 1 September 2020.

Europol, 'Does Crime Still Pay? Criminal Asset Recovery in the EU: Survey of Statistical Information 2010–2014', (July 2016).

Europol, 'From Suspicion to Action: Converting Financial Intelligence into Greater Operational Action', (2017).

Ferwerda, Joras, 'The Economics of Crime and Money Laundering: Does Anti-Money Laundering Policy Reduce Crime?', *Tjalling C. Koopmans Research Institute, Discussion Paper Series 08-35,* (November 2008).

Financial Action Task Force (FATF), 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia Mutual Evaluation Report', (April 2015).

——, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Austria Mutual Evaluation Report', (September 2016).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Belgium Mutual Evaluation Report’, (April 2015).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Canada Mutual Evaluation Report’, (September 2016).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Denmark Mutual Evaluation Report’, (August 2017).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Finland Mutual Evaluation Report’, (April 2019).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Greece Mutual Evaluation Report’, (September 2019).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Hong Kong, China Mutual Evaluation Report’, (September 2019).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Iceland Mutual Evaluation Report’, (April 2018).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Israel Mutual Evaluation Report’, (December 2018).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Italy Mutual Evaluation Report’, (February 2016).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Kingdom of Saudi Arabia Mutual Evaluation Report’, (September 2018).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Mexico Mutual Evaluation Report’, (January 2018).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Norway Mutual Evaluation Report’, (December 2014).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: People’s Republic of China Mutual Evaluation Report’, (April 2019).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Portugal Mutual Evaluation Report’, (December 2017).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Republic of Korea Mutual Evaluation Report’, (April 2020).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Russian Federation Mutual Evaluation Report’, (December 2019).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Sweden Mutual Evaluation Report’, (April 2017).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Switzerland Mutual Evaluation Report’, (December 2016).

——, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Turkey Mutual Evaluation Report’, (December 2019).

——, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: United Arab Emirates Mutual Evaluation Report', (April 2020).

——'Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom Mutual Evaluation Report', (December 2018).

——, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: United States Mutual Evaluation Report', (December 2016).

——, 'Countries', https://www.fatf-gafi.org/countries/, accessed 1 October 2020.

——, 'Guidance for a Risk-Based Approach for Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement', (October 2015).

——, 'Guidance for a Risk-Based Approach: The Banking Sector', (October 2014).

——, 'Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures' (June 2007).

——, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations', (Revised July 2019).

——, 'Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems', (Revised October 2019).

——, 'The Forty Recommendations of the Financial Action Task Force on Money Laundering', 1990.

——, 'Financial Crime: A Guide for Firms. Part 1: A Firm's Guide to Preventing Financial Crime', (July 2016).

——, 'Financial Crime Thematic Reviews: Chapter 4, Automated Anti-Money Laundering Transaction Monitoring Systems (2007)', (Release 48: March 2020).

——, 'Global Financial Innovation Network', https://www.fca.org.uk/firms/global-financial-innovation-network, accessed 15 October 2020.

——, 'The Compliance Function in Wholesale Banks', (November 2017).

Fintech Futures, 'Regional KYC utilities: Genesis of global collaboration on shared compliance platforms', (17 November 2019), https://www.fintechfutures.com/2019/11/regional-kyc-utilities-genesis-of-global-collaboration-on-shared-compliance-platforms/, accessed 20 June 2020.

Giacomini, Paul, Marco Iacano, Jeff Levine, Thomas Messina, Nathan Thomas, 'From Source to Surveillance: The Hidden Risk in AML Monitoring System Optimization', *PwC*, (September 2010).

Halliday, Terence, Michael Levi and Peter Reuter, 'Can the AML system be evaluated without better data?', *Crime, Law and Social Change,* (March 2018), Volume 69, Issue 2, pp. 307–328.

Halliday, Terence, Michael Levi and Peter Reuter, 'Global Surveillance of Dirty Money: Assessing Assessments of Regimes to Control Money-Laundering and Combat the Financing of Terrorism', *Center on Law and Globalization report*, (January 2014).

Haselkorn, Dov, Allen Meyer, Adrian Murphy, Stefano Boezio, 'Finding a Needle in a Haystack: The Case for Rethinking and Upgrading Anti-Money Laundering Transaction Monitoring', *Oliver Wyman* (2017).

Hayday, Matthew, Jan-Alexander Huber, Matthias Memminger, Michael Soppitt, 'How Banks Can Excel in Financial Crimes Compliance', *Bain and Company*, (18 January 2018). See https://www.bain.com/insights/how-banks-can-excel-in-financial-crimes-compliance/.

Heiliczer, Josh, Maggi Hughes, Scott Mandell, David Scott, ''While you monitor transactions, who monitors your transaction monitoring program?', *EY,* (2019).

Her Majesty's Government (HMG), 'Cutting Red Tape review of the Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) regime,' (March 2017).

Hillenius, Giljs, 'Swedish Procurement Study: Web-based Office Tools Not GDPR Compliant', *Open Source Observatory*, (26 February 2019), https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/security-and-compliance, accessed 12 October 2020.

Hong, Austin, Allen Meyer, Adrian Murphy, Alexander Peitsch, Jayant Raman, 'Efficient and Effective Financial Crime Compliance: Dispelling Three Common Myths to Enable Next Generation Solutions' *Oliver Wyman* (2018).

Hong Kong Financial Services Development Council (FSDC), 'Building the Technological and Regulatory Infrastructure of a 21st Century International Financial Centre: Digital ID and KYC Utilities for Financial Inclusion, Integrity and Competitiveness' (June 2018)

Hong Kong Monetary Authority (HKMA), 'AML/CFT RegTech Forum: Record of Discussion', (December 2019).

——'Guidance Paper: Transaction Screening, Transaction Monitoring and Suspicious Transaction Reporting', (Revised May 2018).

——, 'Guideline on Anti-Money Laundering and Counter- Financing of Terrorism (For Authorized Institutions)', (October 2018).

Institute for Electrical and Electronics Engineers' (IEEE) Standards Association, 'Global Initiative on Ethics of Autonomous and Intelligent Systems,' https://standards.ieee.org/industry-connections/ec/autonomous-systems.html, accessed 13 August 2020.

International Institute of Finance (IIF), 'Machine Learning in Anti-Money Laundering – Summary Report', (2018).

IIF & Deloitte, 'The Global Framework for Fighting Financial Crime: Enhancing Effectiveness & Improving Outcomes', (2019).

IReporter, 'Anti-money Laundering Market by Component, Solution, Deployment Mode, End User And Region - Global Forecast to 2025', (September 2020) https://www.reportlinker.com/p05815011/Anti-Money-Laundering-Solution-Market-by-Component-Technology-Type-Deployment-Mode-Organization-Size-And-Region-Global-Forecast-to.html?utm_source=GNW, accessed 1 October 2020.

Jakubowski, Zak, 'Global AML fines reach £540m with reoccurring failures', (10 August 2020), https://www.accountancydaily.co/global-aml-fines-reach-ps540m-reoccurring-failures, accessed 10 September 2020.

Lexis Nexis Risk Solutions, 'True Cost of Financial Crime Compliance Study: Global Report', (March 2020).

Lexis Nexis Risk Solutions, 'True Cost of Financial Crime Compliance Study: European Version', (September 2017).

Liu, Yanan, Jayant Ramen (Oliver Wyman), 'Financial Crime Compliance: Current Global State of Play', *Brink*, (15 October 2017), https://www.brinknews.com/financial-crime-compliance-current-global-state-of-play/, accessed 1 October 2020.

Lopez, Ben, Sabina Munnelly, 'Financial Crime Analytics Utility: Power Together', *Accenture Consulting* (2019).

Maxwell, Nick J., 'Case studies of the use of privacy preserving analysis to tackle financial crime,' *RUSI Future of Financial Intelligence Sharing (FFIS) Innovation and Discussion Paper,* (June 2020).

Maxwell, Nick J., 'Five Years of Growth in Public–Private Financial Information-Sharing Partnerships to Tackle Crime', *RUSI Future of Financial Intelligence Sharing (FFIS) Report*, (July 2020).

Maxwell, Nick J., and David Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', *RUSI Occasional Paper,* (October 2017).

Monetary Authority of Singapore (MAS), 'Guidance for Effective AML/CFT Transaction Monitoring Controls', (September 2018).

Moiseienko, Anton, and Tom Keatinge, 'The Scale of Money Laundering in the UK. Too Big to Measure?', *RUSI Briefing Paper* (February 2019).

Murphy, Adrian, Kate Robu, and Matthew Steinert, 'The Investigator-Centered Approach to Financial Crime: Doing What Matters', *McKinsey and Company*, (May 2020).

Murton, Ramona, 'Keeping an Eye on Suspicious Activity: The Importance of Maintaining Human Analytics', *Association of Certified Anti-money laundering Specialists (ACAMS)*, (2015).

National Crime Agency (NCA), 'National Strategic Assessment of Serious and Organised Crime 2019', (May 2019).

New York Department of Financial Services (NYDFS), 'Superintendent's Regulations: Part 504 – Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications', (January 2017).

Partnership for AI (PAI) Staff, 'PAI Researchers Co-author Multistakeholder Report on Improving Verifiability in AI Development', (15 April 2020), https://www.partnershiponai.org/pai-researchers-co-author-multistakeholder-report-on-verifying-claims-for-ai-development/, accessed 10 May 2020.

Pol, Ronald F., 'Anti-money laundering effectiveness: assessing outcomes or ticking boxes?', *Journal of Money Laundering Control*, (May 2018) 21(2), pp.215-230.

Poncy, Chip, and Juan C. Zarate, 'Designing a New Anti-Money Laundering (AML) System', *Center on Sanctions and Illicit Finance Research Memo,* (September 2016).

Redhead, Matthew, 'Deep Impact? Refocusing the Anti-Money Laundering Model on Evidence and Outcomes', *RUSI Occasional Paper,* (October 2019).

Reuter, Peter, and Edwin M. Truman, *Chasing Dirty Money: the Fight Against Money Laundering*, (Washington, D.C.: International Institute of Economics, 2004).

Sharman, J.C., *The Money Laundry: Regulating Criminal Finance in the Global Economy,* (Cornell University Press: New York, 2011).

Sweeting, Paul, *Financial Enterprise Risk Management,* (Cambridge University Press: Cambridge, 2nd Edition 2017), Chapter 21, pp. 552-572.

The Royal Society, 'Protecting Privacy in Practice: The Current Use, Development and Limits of Privacy Enhancing Technologies in Data Analysis', (March 2019).

The Treasury Alliance Group, 'Fundamentals of Global Payment Systems and Practices', (2018).

The Wolfsberg Group, 'Statement on Effectiveness: Making AML/CTF Programmes More Effective', (December 2019).

Twomey, Niall, 'KYC Utilities: The Second Coming, Learning from Past Failures', *Finextra*, (11February 2020), https://www.finextra.com/blogposting/18446/kyc-utilities-the-second-coming-learning-from-past-failures, accessed 12 March 2020.

United Nations Office on Drugs and Crime (UNODC), 'Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes', *Research Report*, (October 2011).

——, 'Money Laundering and Globalization', https://www.unodc.org/unodc/en/money-laundering/globalization.html, accessed 1 October 2020.

US Federal Financial Institutions Examination Council (FFIEC), 'Bank Secrecy Act/ Anti-Money Laundering Examination Manual', (2014).

US Treasury Financial Crime Enforcement Network (FinCEN), 'Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance', (August 2014).

——, 'FinCEN Announces its Innovation Hours Program', (24 May 2019), https://www.fincen.gov/news/news-releases/fincen-announces-its-innovation-hours-program, accessed 15 October 2020.

——, 'FinCEN Penalizes US Bank Official Corporate Anti Money Laundering Failures', (4 March 2020), https://www.fincen.gov/news/news-releases/fincen-penalizes-us-bank-official-corporate-anti-money-laundering-failures, accessed 10 March 2020.

——, 'FinCEN Provides Further Information to Financial Institutions in Response to the Coronavirus Disease (COVID-19) Pandemic', (2 April 2020), https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-provides-further-information-financial, accessed 10 June 2020.

——, 'Section 314(b) Fact Sheet', (November 2016).

US Treasury Office of the Comptroller of the Currency, 'Supervisory Guidance on Model Risk Management', (April 2011).

Van Duyne, Petrus, 'Serving the Integrity of Mammon and the Compulsive Excessive Regulatory Disorder', *Crime Law and Social Change* 52 (2009), pp.1-8

Vocalink, 'Anti-Money Laundering Solutions. The Rise of the Mule: Identifying Mule Accounts and Tracking Laundered Money', (2017).