Royal United Services Institute
for Defence and Security Studies

Occasional Paper

Deep Impact?

Refocusing the Anti-Money Laundering Model on Evidence and Outcomes

Matthew Redhead

Deep Impact?

Refocusing the Anti-Money Laundering Model on Evidence and Outcomes

Matthew Redhead

RUSI Occasional Paper, October 2019

Royal United Services Institute
for Defence and Security Studies

188 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 188 years.

Published in 2019 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, October 2019. ISSN 2397-0286 (Online); ISSN 2397-0278 (Print).

Printed in the UK by KallKwik.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)

Contents

Acknowledgements

I would like to thank Ernst and Young (EY) and Refinitiv for their financial support of RUSI's Financial Crime 2.0 programme,[1] and all those who generously shared their experience and expertise for this research. I am also grateful to Eric Lorber and David Murray of the Financial Integrity Network (FIN) for reviewing and commenting on a draft of this paper, along with a further anonymous expert who provided extensive comments. Thank you all for your challenges – the paper is better for them, and any faults that remain are mine alone. Thank you too to RUSI's Publications team for their support and patience throughout the editing process.

I would also like to recognise the contribution that Tom Keatinge, Anton Moiseienko and Kayla Izenman made in supporting me throughout the project. They are superb colleagues, and I feel lucky to have worked with them.

1. The Financial Crime 2.0 programme, launched in March 2018, aims to determine how the anti-money laundering (AML) regime needs to be updated to better align with technological innovation.

Executive Summary

THE FINANCIAL ACTION Task Force (FATF), the international standard setter in anti-money laundering (AML), marked its 30th anniversary in June 2019. April 2020 will mark the same anniversary of the first issue of FATF's 40 Recommendations.[1] It is thus an appropriate time to consider their impact.

FATF requires governments and their agencies to implement the standards at a national level, but on a day-to-day basis, the main gatekeepers of the international financial system continue to be the financial services sector. They are therefore the primary point of reference for this paper.

To meet the laws and regulations that have developed in response to the Recommendations, financial institutions (FIs)[2] have invested increasing amounts of money into controls that will ensure 'compliance' with the AML model. Despite substantial levels of private sector investment, however, doubts remain among practitioners and academics about whether the model is effective, not only in terms of how well it is implemented, but in its impact on money-laundering metrics[3] and wider costs and benefits.

Providing answers to these questions currently sits outside FATF's remit as a standard setter. But they remain important questions nonetheless, because there is a considerable discrepancy between most estimates of the scale of money laundering and the levels of disruption and prosecution of money launderers, as evidenced in a 2016 study by the EU policing agency, Europol.[4] Although it is probable that the gap would be wider without the current model, it is impossible to say by how much. It is a problem that deserves proper exploration.

The extent to which the specific AML measures required of FIs impact overall effectiveness is therefore also hard to calibrate. The requirement to file reports on suspicious client activity to national financial intelligence units (FIUs) undoubtedly added value to law enforcement's efforts

1. Financial Action Task Force (FATF), 'The Forty Recommendations of the Financial Action Task Force on Money Laundering', 1990.
2. Financial institutions (FIs) conduct business in one or more of the following areas: accepting deposits; lending, leasing, transferring and exchanging money; means of payment and payment platforms; financial guarantees; trade in foreign exchange, commodities, securities and other monetary instruments; portfolio management; administering funds; investing; and underwriting.
3. FATF defines money laundering as 'the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source', see FATF, 'What is Money Laundering?', 2019, <https://www.fatf-gafi.org/faq/moneylaundering/>, accessed 10 July 2019.
4. Europol, 'Does Crime Still Pay? Criminal Asset Recovery in the EU: Survey of Statistical Information 2010–2014', July 2016.

to identify financial crime.[5] But although there is significant evidence of this requirement's financial cost,[6] there are limited indications to show the scale or significance of its benefits, or how impactful it might be in comparison with other elements of the AML model.

The collective experience of the practitioners interviewed also suggests that the current model is having some degree of impact, but that it is probably not optimal. Negligent implementation aside, a key issue is misaligned incentives. Although several major national regulators are now seeking to take a more flexible approach,[7] regulatory examinations have until relatively recently focused on technical compliance and control failures. Such an approach has led to justifiable censure, fines and reputational damage for cases of FI negligence or criminality.[8] However, a lack of information can also lead an FI to make what turns out to be a 'wrong' risk decision. Unfortunately, the potential punitive risk that goes with being 'wrong' continues to bias the private sector towards over-investment in preventative measures and over-reporting, despite regulatory advice to the contrary. This makes 'real-life' effectiveness for FIs a matter of balancing the costs and risks of regulatory action against the size and efficiency of their compliance functions. The ultimate focus is not therefore on the reduction of money laundering, but on protecting the institution and the bottom line.

The AML model's further fundamental vulnerability is its fragmentation. In the face of increasingly sophisticated, fluid and networked financial crime,[9] AML efforts face a range of operational frictions, between countries, private and public sectors, and individual institutions. Because of this, FIs tend to have a narrow view of who their clients are, and what their behaviour might signify. This makes potential criminality harder to detect.

More positively, recent scandals have encouraged some FIs, regulators and law enforcement agencies to find innovative solutions to the problem of fragmentation. One of the most fundamental changes in FIs has been the growing attempt to transform reactive financial crime 'compliance' cultures into proactive 'risk management'. There are early indications that such efforts, combined with initiatives to increase organisational agility, deploy new technology and improve partnerships with other FIs and the public sector, are improving the efficiency of the current model.

5. National Crime Agency (NCA), 'SARs in Action' (Issue 2, August 2019), p. 20, <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/333-sars-in-action-magazine-august-2019/file>, accessed 11 September 2019.
6. Barney Thompson, 'UK to Sharpen its Tools Against Money Laundering', *Financial Times*, 28 January 2019.
7. See, for example, US Department of Justice Criminal Division, 'Evaluation of Corporate Compliance Programs', April 2019.
8. See, for example, the US DoJ, 'Statement of Facts on HSBC', December 2012, <https://www.justice.gov/sites/default/files/opa/legacy/2012/12/11/dpa-attachment-a.pdf>, accessed 12 January 2019.
9. NCA, 'National Strategic Assessment of Serious and Organised Crime', May 2019, pp. 5, 39–40.

These initiatives remain relatively new, but promising. Regulators thus need to provide rhetorical and practical support: primarily through practical engagement with FIs to identify and share best practice, but also by reinforcing positive commercial and reputational incentives for the private sector.

In the longer term, some experts have suggested a more radically integrative agenda to improve AML effectiveness, pooling data and expertise within the private sector, and between the private and public sectors.[10] This agenda might have benefits in reducing fragmentation and duplication of effort, but such a radical shift is not without problems of its own – not least which sector, public or private, should take ownership and leadership.

Either way, an evidence-based approach demands that before making such decisions there needs to be consistent research to suggest that an integrated model has measurable benefits over and above the current framework. Better evidence is the most pressing need.

Recommendations

Recommendation 1: FATF member governments should create or designate a permanent mechanism for improving the evidence base on the impact, costs and benefits of the current AML framework.

Recommendation 2: Regulators and law enforcement should work with FIs to better align inter-institutional incentives on the objective of reducing financial crime.

Recommendation 3: Regulators should identify and share best practice with peers and the private sector on improving organisational agility in FI financial crime risk management.

Recommendation 4: Regulators and law enforcement should identify and share best practice with peers and the private sector on integrating financial intelligence into FIs' financial crime risk-management structures.

Recommendation 5: Regulators and law enforcement should continue to encourage, protect and evaluate FI technological innovation for detecting financial crime risk at all stages of the client life cycle.

Recommendation 6: Regulators and law enforcement should continue to expand legal and technical frameworks for fostering financial intelligence sharing in and between both the public and private sectors.

Recommendation 7: Governments, regulators and industry associations should work with FIs to ensure that the benefits of innovation are shared equally across the private sector.

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

Recommendation 8: In the medium term, governments and regulators should explore the costs and benefits of a more unified approach than the current model, whether under public or private sector leadership.

Introduction

THIS PAPER EXAMINES the effectiveness of the current anti-money laundering (AML) model, with particular reference to the financial services sector. The objectives of the paper are to:

- Outline the current AML model and its implications for financial services.
- Explore the meaning of effectiveness in AML and discuss whether the model is currently effective.
- Explore ways in which the financial services sector, regulators and law enforcement have sought to make the model more effective.
- Look forward to future developments which might further enhance the model's effectiveness.
- Make relevant recommendations to enhance the model's future effectiveness. The paper is structured into four chapters that cover these objectives in sequence.

Chapter I outlines the financial services sector's two key roles in the AML model – to take necessary and proportionate efforts to:

- Prevent the financial system from being used for criminal purposes.
- Detect and report potential criminal activity to support law enforcement.

Laws and regulations framed by the Financial Action Task Force's (FATF's) Recommendations require financial institutions (FIs) to meet these obligations through an array of policies, procedures and controls, such as customer due diligence (CDD) and 'know your customer' (KYC) requirements, screening, transaction monitoring, and issuing suspicious activity reports (SARs).[1]

Chapter II explores what 'effectiveness' means in the model, both strategically and for FIs. FATF's current approach is to see effectiveness as an assessment of how well its Recommendations have been implemented, an approach which translates down to how national regulators assess FIs. In the language of evidence-based research, this is programme effectiveness – not outcome or cost effectiveness. It does not consider the scale of impact compliance will have on the policy's target – financial and predicate crimes – or the policy's wider costs and benefits. As a result, there is limited evidence on which to judge the model's overall anti-financial crime effect.

Because of this focus on programmatic effectiveness, FIs tend to focus on technical compliance and sufficient investment in people, processes and technology to minimise the number and

1. Suspicious activity/transaction/matter reports are reports of suspicions of money laundering, terrorist financing or proliferation financing made by regulated entities to their national financial intelligence unit. For simplicity, in this paper all such reports are referred to as SARs.

significance of inevitable control failures. This in turn encourages FIs to think of effectiveness as a matter of warding off regulators while taming compliance costs. Reducing money laundering and predicate crimes is not a primary incentive and is hoped to occur as a welcome by-product of implementation.

Chapter II also explores why some practitioners and academics believe that the model might not be as impactful as it could be because of its fragmentation. There is a huge division and duplication of labour between many agencies in the public sector, and between institutions in the private sector. FIs only have a narrow view of the risks they face, and yet are required to take credible action to prevent and report potential criminality. Although FATF, regulators and law enforcement agencies (LEAs) produce steady streams of guidance on the implementation of policy and changes in criminal modus operandi,[2] such guidance tends to lag behind changes in criminal technique.

Chapter III explores how a desire to address AML failures, poor incentives and the fragmentation of the model have led to new thinking in both the public and private sectors. For FIs, this shifting atmosphere has fostered a number of initiatives to reduce further reputational and regulatory risk, improve cost effectiveness, and deliver stronger AML leads and outcomes to regulators and LEA. These initiatives fall into four themes:

- Integration and cultural change in financial crime risk and compliance functions.
- Development of intelligence functions as a supplement to existing controls.
- Technology and new data analytic techniques supported by machine learning to identify risk more accurately.
- Partnerships between FIs and the public sector to improve information sharing.

These initiatives are all relatively new. Although innovating FIs have faced challenges in making structural changes, using financial intelligence and deploying new technology, initial indications are positive, especially when viewed in combination with the benefit of closer public–private partnerships.

The final chapter considers where these current trends will lead next. The consensus of practitioners is that these initiatives will continue, and possibly be extended, with greater data sharing and operational cooperation between the sectors over time. Evidence-based policy research will need to be a key part in assessing the impact of these innovations. Sector-wide initiatives will also be needed to ensure that all FIs – not just the wealthiest – can benefit from innovation. Those who attended a RUSI-hosted workshop and were interviewed individually universally perceived an increasingly fluid and networked AML response to be the best way to improve both cost and outcome effectiveness in the long term. However, uncertainties remain about how this ‘end state’ could be achieved, and whether the main impetus should come from the public or the private sectors.

2. For examples of such documents, see FATF, ‘Guidance’, <http://www.fatf-gafi.org/documents/guidance/?hf=10&b=0&s=desc(fatf_releasedate)>, accessed 23 August 2019.

Methodology

The paper is based on a literature review of publicly available information, including academic and policy research, government documents, and reports from international bodies such as FATF and the IMF. In addition, the author conducted 30 semi-structured interviewers with financial crime risk professionals with regulatory, law enforcement, government and private sector experience. To discuss initial findings, RUSI's Centre for Financial Crime and Security Studies held a workshop in London on 29 April 2019, with 26 representatives from across these sectors.

Caveats

The AML institutional framework covers an increasing range of obligated sectors in the private sector, international organisations, national regulators and LEAs. This paper does not seek to assess all those elements but has a primary focus on the financial services. It also focuses on money laundering, as opposed to other financial crimes such terrorist financing. Nonetheless, the report still speaks to issues of compliance and effectiveness that affect other obligated sectors and different types of financial crime.

I. The AML Model

THE ROOTS OF the modern approach to anti-money laundering lie in the 1980s, where concern among major developed countries about the scale of the illegal drugs trade led to concerted efforts to undermine its financial incentives. In 1988, the UN agreed its Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, and the Basel Committee on Banking Supervision issued its statement on money laundering.[3] The following July, at the Group of Seven meeting in Paris,[4] the group's heads of government, along with the president of the European Commission, took the further step of creating an intergovernmental group, FATF, to create agreed standards on combating money laundering arising from the sale of drugs.

The FATF 40 Recommendations

Scope

In April 1990, FATF issued the first version of what have become known as the '40 Recommendations', a set of universally applicable AML measures for governments and agencies, with significant implications for banking and other financial services. The Recommendations have been revised four times since, most recently in February 2012, when the nine special recommendations were integrated fully into the 40 Recommendations.[5] In these changes, FATF widened its coverage of:

- **Obligated entities**, to include non-banking FIs and more recently, designated non-financial businesses and professions (DNFBPs) such as lawyers and real-estate agents.[6]
- **Offence types**, which now include a wider range of predicate money-laundering offences, such as fraud and human trafficking, as well as other financial crimes, such as terrorist financing and weapons of mass destruction proliferation.[7]

---

3. UN, 'United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances', 1988; Basel Committee on Banking Supervision, 'Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering', December 1988.
4. The Group of Seven includes France, Germany, the UK, Italy, Japan, the US, and Canada.
5. FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations', February 2012, updated June 2019.
6. Designated non-financial businesses and professionals (DNFBPs) include casinos, real-estate businesses, dealers in precious metals and stones, lawyers and accountants, and trust and company service providers.
7. This paper uses the terms 'money laundering' and 'financial crime' synonymously. However, properly speaking, financial crime refers to a broader range of offences, including terrorist financing and sanctions evasion.

As FATF's scope has grown, so too has the global credibility of its Recommendations. From its original 16, FATF now comprises 37 member states, two member regional organisations, and nine FATF-Style Regional Bodies, with over 200 jurisdictions now committed to meeting the Recommendations.[8]

Evaluation Role

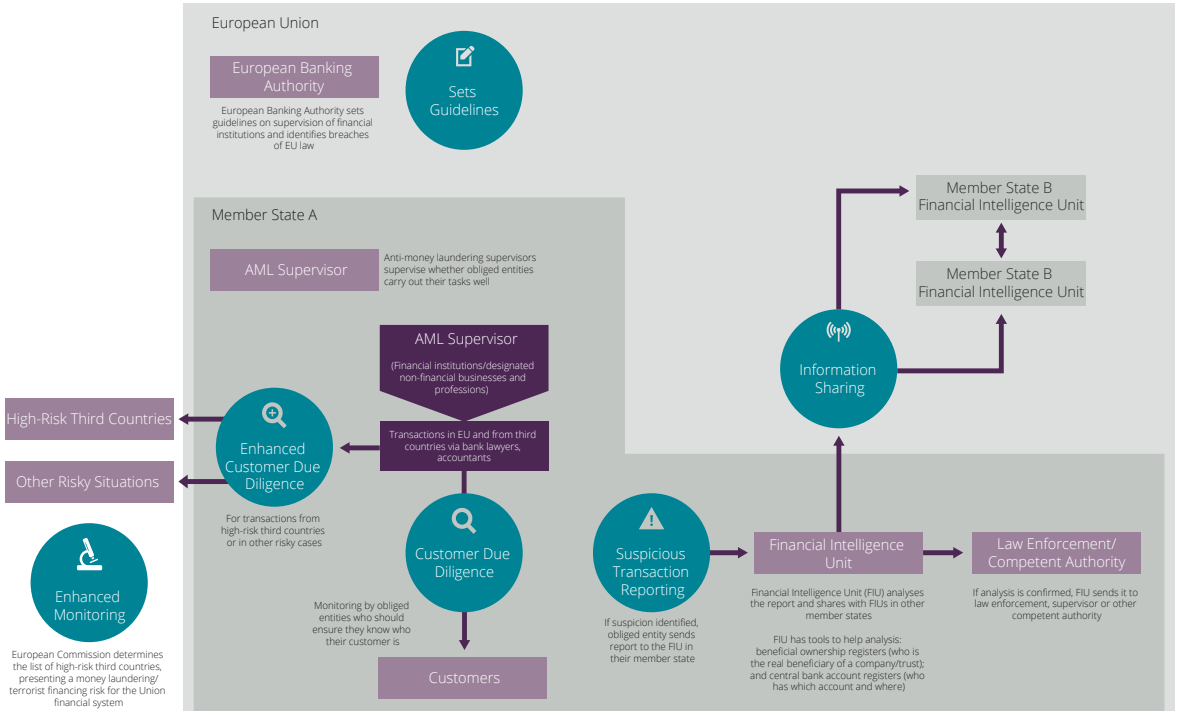
The underlying assumption of the Recommendations is that compliance is a necessary prerequisite to preventing and/or detecting money laundering, but not a perfect one. FATF therefore accepts that full implementation is aimed at the mitigation rather than elimination of money laundering. In terms of national performance assessment, FATF oversees periodic mutual evaluation reports (MERs) of member states' performance. The fourth round of evaluations, based on the 2012 Recommendations, began in 2014, and is expected to be completed in the early 2020s. Previous rounds have focused primarily on technical compliance, but there has been a greater emphasis on evidencing the effective implementation of the Recommendations, which is discussed in Chapter II.[9]

EU Case Study

Member jurisdictions are expected to implement the Recommendations as a minimum standard, setting in place laws and regulations founded upon them. In the EU, for example, the FATF framework has helped frame successive AML directives (AMLDs), the first of which came into force in April 1994, and the most recent of which – the fifth – is to be transposed into national laws by January 2020.[10] The AMLDs have built upon the minimum standards of the Recommendations, becoming increasingly directive over time, but still leaving some discretionary scope for implementing the Recommendations in different national contexts. The supranational and national AML structure within EU member states illustrates the key elements of the FATF model (see Figure 1), with obligated entities such as FIs observed by a national AML supervisor or regulator, fulfilling due diligence requirements and reporting suspicious activity to a national FIU.

8. FATF, 'Countries', <https://www.fatf-gafi.org/countries/>, accessed 29 April 2019; FATF, 'FATF Members and Observers', <https://www.fatf-gafi.org/about/membersandobservers/>, accessed 29 April 2019.
9. FATF, 'Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems', updated February 2019.
10. European Parliament and Council of the European Union, 'Directive (EU) 2018/843 of the European Parliament and of the Council', *Official Journal of the European Union* (L156/43, 30 May 2018).

Figure 1: AML Structures in the EU



Source: European Commission, 'Preventing Money Laundering and Terrorist Financing Across the EU. How does it Work in Practice?', 2018, <https://ec.europa.eu/info/sites/info/files/diagram_aml_2018.07_ok.pdf>, accessed 3 January 2019.

The Recommendations and Financial Services

Section D of the Recommendations (numbers 9–21) places responsibilities on FIs and other obligated entities to take reasonable efforts to:

- **Prevent the criminal misuse of their services**: FIs are expected to understand the risks around their relationship with an individual or business. In the event that there are material financial crime risks, providers are expected to make informed decisions about whether to 'onboard' or retain them. These requirements are covered by Recommendations on CDD (10–11), due diligence for particular types of higher-risk customer (12–16), and the use of third parties to deliver these services (17–19).[11]
- **Detect and report suspicious activity**: FIs should identify potentially suspicious financial behaviour and send credible SARs to the national financial intelligence unit (FIU), to support investigations of financial and predicate crimes. FIs are also expected to act promptly to requests for information. This requirement is covered by Recommendations 20 and 21.[12]

11. FATF, 'The FATF Recommendations', pp. 12–17.
12. *Ibid*., p. 17.

The Recommendations and the laws and regulations that have flowed from them are largely not prescriptive about how these requirements are met. However, they have inexorably shaped the key elements of a common financial crime compliance function in FIs, as outlined in Tables 1 and 2 below.

Table 1: Measures to Exclude and Identify Potential Financial Crime

CDD/KYC	Enhanced Due Diligence (EDD) for High-Risk Customers	Customer and Transaction Screening
FIs undertake identification and verification (IDV) procedures and identify the purpose and nature of business and 'beneficial owners' (BO) for commercial relationships. CDD/KYC data is subject to both regular review and review following 'trigger events' such as the issue of a SAR.	'High-risk' clients, such as 'politically exposed persons' (PEPs), go through further stages of due diligence, background checks and identification of sources of funds to verify a low financial crime risk. EDD data is subject to more regular review than CDD.	New clients are screened against sanctions, terrorist and other watch lists, and periodically when those lists are updated. International payments are also screened. Validated 'true matches' are self-reported to the relevant national government agency, such as the Office for Foreign Assets Control (OFAC) in the US.

Source: The author.

Notes: FATF defines a BO as a 'natural person(s) who ultimately owns or controls a customer', see FATF, 'Transparency and Beneficial Ownership', October 2014, p. 8. How this is defined in terms of ownership/control can vary between jurisdictions. In the UK, 'Persons of Significant Control' have 25% or more of shares/voting rights.

FATF defines a PEP as 'an individual who is or has been entrusted with a prominent function', see FATF website, <https://www.fatf-gafi.org/documents/documents/peps-r12-r22.html>, accessed 11 September 2019.

Table 2: Measures to Detect and Report Potential Financial Crime

Transaction Monitoring	Triage and Escalation	Investigation/Reporting Teams
Most FIs use automated platforms to identify potentially suspicious behaviour. Conventionally, these systems use rules-based analysis, where if a given scenario occurs (for instance, a client pays in multiple cash deposits in round figure amounts), the system will send an alert.	Alerts are usually checked by analysts at different levels for potential misreporting, usually based on varying levels of analysis of contextual account behaviour. Over these stages, the majority of alerts are usually rejected as false positives.	At the final stage, a team of human analysts/investigators will come to a decision as to whether the alert and subsequent contextual investigations amount to potentially suspicious activity. If so, a report is issued to the national FIU.

Source: The author.

The size and design of these elements vary greatly depending on a range of factors such as an FI's size, profitability, age, culture(s), geographic footprint, product range, client base, and overall risk profile. For example, larger and older institutions tend to have larger functions and a greater investment in multiple legacy systems, while the financial technology (FinTech) sector has tended to experiment with smaller, lighter and more technologically agile processes, especially in KYC. These elements – sometimes in combination with other aspects of regulatory compliance – usually sit in one of three locations within FIs beneath or as part of the legal department or risk function, or in some cases have a stand-alone existence and a seat at the board, as illustrated in Figure 2.

Figure 2: Compliance Organisational Positions

Source: Piotr Kaminski and Kate Robu, 'A Best-Practice Model for Bank Compliance', McKinsey and Company, January 2016, <https://www.mckinsey.com/business-functions/risk/our-insights/a-best-practice-model-for-bank-compliance>, accessed 12 February 2019.

Three Lines of Defence (TLoD)

Beyond FATF requirements, most FIs have sought to conceptually segment their financial crime compliance functions with what has become known as the 'Three Lines of Defence' (TLoD), an approach widely applied in financial services risk management (see Box 1).[13]

13. Howard Davies and Maria Zhivitskaya, 'Three Lines of Defence: A Robust Organising Framework, or Just Lines in the Sand?', *Global Policy* (Vol. 9, Supplement 1, June 2018), p. 37.

Box 1: Defining the Three Lines of Defence (TLoD)

- The First Line of Defence (1LoD) is the day-to-day implementation of policies, procedures, controls and risk-management frameworks.
- The Second Line of Defence (2LoD) is the oversight and development of policies, procedures, controls and risk-management frameworks.
- The Third Line of Defence (3LoD) is the assurance and audit of the implementation, oversight and development of those policies, procedures, controls and risk-management frameworks.

According to the UK's Financial Conduct Authority, all of the 22 wholesale banks in a sample study in 2017 used the TLoD, typically defining financial crime compliance as a 2LoD function.[14] Paul Sweeting, an expert in risk management, has identified three 'styles' of interaction that are combined with the TLoD:

- **Offence and Defence**: 1LoD is completely commercial and has an antagonistic relationship with its compliance or risk-management functions.
- **Policy and Policing**: 2LoD creates the framework that 1LoD implements and 'owns' the residual risks; 2LoD then polices 1LoD implementation.
- **Partnership**: 1LoD and 2LoD work together in a cooperative way to ensure the development and exploitation of commercial opportunities within risk appetite and regulatory bounds.[15]

Based on interviews, it appears that most large institutions follow the 'policy and policing' style, although some practitioners provided anecdotal reports of outright opposition between 1LoD and 2LoD. 'Partnership' was often described in more aspirational terms, and some noted the risk of either of the first two lines 'going native' if working together too closely.[16]

14. Financial Conduct Authority (FCA), 'The Compliance Function in Wholesale Banks', November 2017, p. 6.
15. Paul Sweeting, *Financial Enterprise Risk Management,* 2nd Edition (Cambridge: Cambridge University Press, 2017), pp. 552–72.
16. Author telephone interview with former senior regulator and compliance professional, 18 February 2019 (hereafter 'Interview A'); author interview with senior compliance official and financial crime risk consultant and auditor, London, 21 February 2019 ('Interview B'); author interview with senior financial crime transformation expert, London, 28 January 2019 ('Interview C').

II. The Effectiveness of the Model

THE QUESTIONS OF whether this AML model does work or can work have become increasingly vexed, if not least because the concept of what 'success' amounts to has not always been clear.

The Problem of Defining 'Effectiveness'

FATF is primarily a standard setter and its notion of effectiveness is therefore linked to whether, and how well, its Recommendations are applied. In its initial national mutual evaluations, FATF considered only technical compliance with the Recommendations. This was later revised in 2003, when it was accepted that the implementation of some measures could vary depending on the inherent risk of certain geographies, customer and product types, and delivery channels.[17] In 2007, FATF issued a guidance document on the risk-based approach,[18] followed by further specific guidance for different sectors.[19] FATF further revised its Recommendations in 2012, and adopted a new assessment methodology in 2013, to include an equal focus on what it termed 'effectiveness', based on a three-level hierarchy.[20]

17. FATF, 'The Forty Recommendations', June 2003, p. 3.
18. FATF, 'Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures', June 2007.
19. For a recent example, see FATF, 'Guidance for a Risk-Based Approach for Legal Professionals', June 2019.
20. FATF, 'An Effective System to Combat Money Laundering and Terrorist Financing', <https://www.fatf-gafi.org/publications/mutualevaluations/documents/effectiveness.html>, accessed 8 January 2019.

Box 2: FATF's Objectives and Outcomes

- A 'high-level objective': ensure 'financial systems and the broader economy are protected from the threats of money laundering and the financing of terrorism and proliferation, thereby strengthening financial sector integrity and contributing to safety and security'.

- Three 'intermediate outcomes': 1) lessen overall money laundering and counterterrorist financing risks; 2) detect the proceeds of crime and keep funds out of the financial system; and 3) detect money-laundering threats, deprive criminals and terrorists of illicit funds, and prevent terrorist acts.

- 11 'immediate outcomes', providing operational objectives for direct evaluation.

Source: FATF, 'An Effective System to Combat Money Laundering and Terrorist Financing', <https://www.fatf-gafi.org/publications/mutualevaluations/documents/effectiveness.html>, accessed 8 January 2019.

Immediate Outcome 4 (IO4) is most squarely focused on obligated entities, stating that 'financial institutions and DNFBPs … [should] … adequately apply AML/[CTF] preventive measures commensurate with their risks, and report suspicious transactions'.[21] It recommends that evaluation of effectiveness here should focus on six core issues:[22]

- An understanding of the institutions' financial crime risks and obligations.
- The application of commensurate risk-management measures.
- Appropriate CDD and record-keeping.
- Appropriate measures to manage high risks such as PEPs, new technology and sanctions breach risks.
- Appropriate internal controls and procedures.
- Appropriate suspicious activity reporting.

Potential supporting information to make an assessment included institutions' internal reporting of risks and trends, policies and procedures, examples of failures, internal quantitative measures such as frequency of reviews, training, and time efficiency of systems used to undertake CDD, monitoring and suspicious activity reporting.[23] FATF issued a guidance note on relevant data and statistics that could be collected to support the evaluation of all the objectives in October 2015.[24]

21. FATF, 'Methodology', p. 103.
22. *Ibid*., p. 104.
23. *Ibid.*, p. 105.
24. FATF, 'Guidance: AML/CFT-Related Data and Statistics', October 2015.

Reviewing FATF's Methodology

FATF's shift away from a 'tick-box' approach has been welcome. However, its current Methodology still takes a narrow view of effectiveness. Most methodologies of evidence-based policy research typically identify three types of effectiveness (though sometimes using differing nomenclature).[25]

Box 3: Defining Effectiveness

- Programme effectiveness: The evaluation of whether the policy is having a net effect on beneficial activities and behaviours that would not have occurred without the policy.
- Outcome effectiveness: The evaluation of whether the policy has had a net effect on the scale or character of the policy issue or problem that would not have occurred without the policy.
- Cost effectiveness: The evaluation of the costs and externalities of the policy, which need to be set against the resource inputs and outcomes achieved in order to conclude whether the policy is producing 'value for money' and is not potentially generating more problems than it potentially solves.

Source: Ronald F Pol, 'Anti-Money Laundering Effectiveness: Assessing Outcomes or Ticking Boxes?', Journal of Money Laundering Control *(Vol. 21, No. 2, 2018).*

At best, the Methodology aims at the evaluation of programme effectiveness, although as Ronald Pol has recently argued, the Immediate Outcomes themselves are 'often ambiguous, unrealisable or lacking measurability' and the kinds of statistics and data required to support evaluation have much in common with 'process or output measures'.[26] As Pol and other academics have noted, the Methodology lacks the key elements needed to assess outcome or cost effectiveness,[27] including:

- **An assessable overall objective**, such as the reduction of the volume of money laundering, proceeds of crime (PoC), predicate offences or societal harms.

25. See, for example, US Government Accountability Office, 'Performance Measurement and Evaluation: Definitions and Relationships', May 2011.
26. Ronald F Pol, 'Anti-Money Laundering Effectiveness: Assessing Outcomes or Ticking Boxes?', *Journal of Money Laundering Control* (Vol. 21, No. 2, 2018), p. 221.
27. Terence Halliday, Michael Levi and Peter Reuter, 'Can the AML System be Evaluated Without Better Data?', *Crime, Law and Social Change* (Vol. 69, No. 2, 2018), pp. 307–28; Pol, 'Anti-Money Laundering Effectiveness'; J C Sharman, *The Money Laundry: Regulating Criminal Finance in the Global Economy* (New York, NY: Cornell University Press, 2011), p. 20.

- **A theory of change or logic model**, to explain why and how the Recommendations should work, and when. As Jason Sharman notes, the model does indeed have a 'common sense' appeal: 'crime is profit driven, so reducing profits will reduce crime'.[28] But this assumption has not been empirically tested by FATF itself.
- **An understanding of costs**, benefits and externalities generated by the systems.
- **A methodology** for data collation and analysis on outcome and cost effectiveness.

Between 1996 and 2000, FATF did work on some of these issues, in particular the scale of money laundering, but research reportedly foundered over what was to be measured. Some member governments wished to use a broad PoC measurement, including all funds generated by predicate offences, whether directly laundered through dedicated schemes or indirectly laundered through immediate spending or reinvestment in criminal activities, while others wanted to count only criminal funds that were directly laundered.[29] This disagreement led to a failure to arrive at an accepted figure for money laundering, or a shared methodology for calculating it.

In theory, the national money-laundering risk assessments required by FATF should give a 'rough and ready' indication of whether the scale of money laundering in a country is changing over time.[30] However, even where countries have undertaken such assessments, the figures are general and often do not change; for example, the 2018 US National Money Laundering Risk Assessment restated the figure of $300 billion generated annually in illicit proceeds in the US, a figure first provided in the 2015 report.[31] As a result, the AML community tends to lack not only reliable estimates of the scale of money laundering or PoC, but also a sense of whether it is going up or down in response to action.[32]

This can create apparently paradoxical situations, especially when the results of MERs are set against estimates of the scale of national money laundering. For example, the UK's 'National Strategic Assessment of Serious and Organised Crime 2019' repeated the previous year's estimate that the volume of money laundering in the UK was in the 'hundreds of billions of pounds'.[33] However, the FATF's fourth mutual evaluation of the UK's AML/CTF framework, published in December 2018, assessed that the UK had 'implemented an AML/[CTF] system that

28. Sharman, *The Money Laundry,* p. 20.
29. *Ibid.,* p. 19.
30. FATF, 'Guidance: National Money Laundering and Terrorist Financing Risk Assessment', 2013.
31. US Department of Treasury, 'National Money Laundering Risk Assessment 2015', 2015, p. 2; US Department of Treasury, 'National Money Laundering Risk Assessment 2018', 2018, p. 2.
32. To note, other international organisations such as the UN Office on Drugs and Crime (UNODC), the IMF and the World Bank have been undertaking academic research on the scale of one portion of global money laundering – international illicit flows – for some time. See UNODC, 'Second Expert Meeting on Statistical Methodologies for Measuring Illicit Financial Flows', 20–22 June 2018, <https://www.unodc.org/unodc/en/data-and-analysis/statistics/Expert-Meeting-Measuring-Illicit-Financial-Flows.html>, accessed 23 August 2019.
33. NCA, 'National Strategic Assessment of Serious and Organised Crime 2019', May 2019, p. 39.

is effective in many respects'.[34] Although it is likely that the total amount of money laundering in the UK would be higher without any AML controls, there is no way of knowing by how much. Either way, it cannot be said with certainty that a framework which still results in the laundering of hundreds of billions of pounds annually is optimally effective.

Assessing Effectiveness

Nonetheless, this lacuna has not prevented academics and researchers from developing some of the basic logic and metrics that would help develop a sense of outcome effectiveness, initially at a macro level. Global estimates, based on discrepancies in global capital flows, trade mis-invoicing, and discrepancies between multinational companies' declared profits and assets, have led to a range for the scale of global money laundering somewhere between 2% and 5% of global GDP.[35] Several years ago, Alberto Chong and Florencio López-de-Silanes also produced a national 'dashboard' approach, using six 'hard' and 'soft' criteria, including estimates of a jurisdiction's underground economy as well as subjective indicators from opinion surveys.[36] Recently in the UK, RUSI also provided a brief overview of possible methodologies to estimate national PoC.[37] Despite the methodological problems that face measurement of money laundering, there appears to be ample scope for researching this issue further.

The same can also be said of understanding the economic logic of money laundering. Joras Ferwerda has suggested that increasing the transaction costs of money laundering can be shown to have had a modest dampening effect on the scale of money laundering and underlying predicate crimes in some jurisdictions.[38] Nonetheless, other researchers have questioned the robustness of his approach,[39] indicating that more research is required for a consensus view to develop. In the interim, therefore, there is no strong evidential basis to show the extent to which the AML framework's implementation affects the scale of money laundering.

A key proxy barometer for overall programme effectiveness should be SAR reporting, because it is a potential measure of criminal activity identified. However, there are difficulties in comparing national and institution-level SAR volumes and reporting data because of variations in thresholds and risk appetite not only between countries, but also between FIs, and even within some of the largest multinational FIs. In the US, for example, investigators tend to have a

34. FATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom Mutual Evaluation Report', December 2018, p. 5.
35. See Halliday, Levi and Reuter, 'Can the AML System be Evaluated Without Better Data?', p. 6.
36. Alberto Chong and Florencio López-de-Silanes, 'Money Laundering and its Regulation', *Economics and Politics* (Vol. 2, No. 1, March 2015), pp. 78–123.
37. Anton Moiseienko and Tom Keatinge, 'The Scale of Money Laundering in the UK: Too Big to Measure?', RUSI Briefing Paper, February 2019.
38. Joras Ferwerda, 'The Economics of Crime and Money Laundering: Does Anti-Money Laundering Policy Reduce Crime?', Discussion Paper Series 08–35, Tjalling C Koopmans Research Institute, November 2008, pp. 15–16.
39. Sharman, *The Money Laundry*, pp. 41–42.

low threshold of suspicion in comparison to European jurisdictions.[40] Filing institutions can also be more or less conservative, often depending on whether the institution has been subject to previous regulatory censure for poor controls.[41]

In addition, although SARs are often valuable for trend analysis and as an investigative database, they are of variable quality as immediate investigative leads. In a RUSI workshop in 2017, one national FIU represented reported that 97% of SAR information they received had no immediate value to their investigations. Moreover, linked surveys conducted with 135 financial crime professionals in Hong Kong, Singapore and Argentina found that across the surveys, 85–95% of participants disagreed or strongly disagreed with the view that SARs lead to the effective discovery and disruption of crime.[42] In interviews conducted for this paper, former senior officials suggested that no more than 1–2% of conventional SARs were likely to be of immediate investigative value for LEAs.[43]

Although it is far from being the only factor, it is likely that this poor quality of lead material plays a role in the poor current rates of freezing or seizure of criminal assets. In 2012, the UN Office on Drugs and Crime estimated that less than 1% of criminal funds flowing through major economies and offshore centres every year is seized and frozen,[44] while in 2016, Europol estimated that between 2010 and 2014, only 2.2% of the estimated PoC in the EU were provisionally seized or frozen, and only 1.1% ultimately confiscated.[45] This further raises the question of how cost effective such a framework can be, especially for smaller FIs and developing jurisdictions.[46]

Based on what is currently known, therefore, one can only state that the AML requirements are likely to have some positive effect at a macro level, but there is no consensus idea of how much, why, or whether other alternative approaches might not have a greater effect. The AML model may well also have significant unknown costs and externalities.[47] It also is not known how significant the AML requirements of obligated entities are vis-à-vis other elements of the model, such as government investment in LEAs.[48] As one interviewee commented, it is

40. Halliday, Levi and Reuter, 'Can the AML System be Evaluated Without Better Data?', p. 12.
41. Interview A.
42. Nick J Maxwell and David Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', *RUSI Occasional Paper* (October 2017), p. vi.
43. Interview A; author interview with former senior law enforcement official and senior compliance professional, London, 14 March 2019 ('Interview D'); author interview with former senior law enforcement official, London, 8 March 2019 ('Interview E').
44. UNODC, 'Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes', Research Report, October 2011, p. 11.
45. Europol, 'Does Crime Still Pay? Criminal Asset Recovery in the EU: Survey of Statistical Information 2010–2014', July 2016.
46. Sharman, *The Money Laundry*, pp. 53–57.
47. Petrus C van Duyne, 'Serving the Integrity of Mammon and the Compulsive Excessive Regulatory Disorder', *Crime, Law and Social Change* (Vol. 52, No. 1, 2009), pp. 1–8.
48. Author telephone interview with former senior regulator, 19 March 2019 ('Interview L').

an untested assumption that FIs play the most important role in AML,[49] and in the absence of more detailed research, it is not possible to make a more credible judgement. It is conceivable, as another interviewee suggested, that some of the AML model's possible difficulties might be more effectively mitigated by changes that occur outside their sphere of responsibility, such as through the radical improvement of corporate transparency.[50]

Implications for Financial Services

FATF's IO4 asserts that the implementation of the Recommendations in FIs and other obligated entities 'ultimately leads to a reduction in money laundering and terrorist financing activity within these entities'.[51] As with other parts of the framework, the assumption is that preventative and disruptive measures contribute to 'outcome effectiveness', but there is no detail as to how much, or why. More to the point, it is not the main focus of evaluation of FI performance. Following the FATF approach, regulators have tended to evaluate an institution's effectiveness on technical compliance and, as the Methodology suggests, the regulators' subjective judgement of 'how well' – or not – those requirements have been implemented, as evidenced in regulatory manuals.[52] In effect, this is a partial evaluation of institutional programme effectiveness alone.

Several significant national regulators are exploring innovative approaches to financial crime regulation, through international collaboration such as the Global Financial Innovation Network (GFIN), a group of 38 national regulators founded in January 2019,[53] and supportive policy statements, such as the US inter-agency 'Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing' of December 2018.[54] According to three interviews with senior compliance professionals who had previously been senior regulators and/or law enforcement officials, regulatory interest in how well FI investigations contribute to the disruption of money laundering is also improving.[55] However, the consensus testimony of officials at the RUSI workshop suggests that positive attitudes towards innovation at a senior regulatory level are taking time to work through into the practice of regulatory examinations,

49. Interview B.
50. Author interview with financial journalist, London, 7 February 2019 ('Interview M'); Sharman, *The Money Laundry*, pp. 68–95.
51. FATF, 'Methodology', p. 103.
52. *Ibid*., p. 104; see also, for example, US Federal Financial Institutions Examination Council (FFIEC), 'Bank Secrecy Act/Anti-Money Laundering Examination Manual', 2014.
53. For the Global Financial Innovation Network membership and scope, see FCA, 'Global Financial Innovation Network', <https://www.fca.org.uk/firms/global-financial-innovation-network>, accessed 23 August 2019.
54. Board of Governors of the Federal Reserve System (FRS) et al., 'Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing', 3 December 2018.
55. Author interviews with three compliance professionals: London, 8 February 2019; telephone, 25 February 2019; London, 14 March 2019.

even in an innovation leader such as the UK.[56] The London-based workshop told a similar story of examinations typically comprising:

- **Literature reviews** of policy, procedure, processes and system-based control documentation, model governance for transaction monitoring, screening and other technical solutions, management information and statistics on false positive rates and SAR volumes.
- **Interviews** of staff in various functions and grades to test their knowledge and practical experience of implementation of policies and procedures, identifying gaps in implementation.
- '**Mini-inquests**' into self-identified issues in onboarding, monitoring, screening and reporting processes, along with further random sample file reviews and ad hoc reviews of control failures.

A Problem of Incentives

Examinations thus continue to focus more on 'what is missing' and 'what has gone wrong'.[57] A 'glass half empty' approach can at least demonstrate institutional AML programme ineffectiveness, especially as the result of negligence and/or malfeasance. There are numerous recent case studies of both; reports on the Global, Azerbaijani and Troika Laundromat money-laundering schemes over the last three years have shown the important role that some banks in Russia, the Baltic states and Scandinavia played, largely by 'turning a blind eye', but also in some instances, as with the Russian bank Troika Dialog, by allegedly being actively involved.[58]

However, such examples of negligence or malfeasance are not always a sufficient explanation for why systems do not work. As regulators are making increasingly clear, they understand that non-systematic failures do occur, and there is a preference for not censuring one-off mistakes.[59] However, FIs are not all confident that this will happen, leading to a persistent 'insurance mentality'. In the face of this interrogative bias in the system, FIs are incentivised to focus on technical compliance and the demonstration of an absence of significant failures, which can lead to significant financial investments in people and systems. Recent industry surveys have suggested that compliance spending among FIs has escalated over recent years, and although

56. RUSI workshop on 'Financial Crime 2.0 – Compliance and Effectiveness', London, 29 April 2019.
57. The FCA is seeking to put an equal stress on good as well as bad practice. See FCA, 'Financial Crime: A Guide for Firms. Part 1: A Firm's Guide to Preventing Financial Crime', July 2016.
58. The Organized Crime and Corruption Reporting Project has been a lead player in the investigation of these schemes. For ongoing details of these investigations, such as 'The Troika Laundromat', see <https://www.occrp.org/en/troikalaundromat/>, accessed 20 June 2019; for more historic failures, see also *Fintech Times*, 'Global Financial Institutions Fined $26 Billion for AML, Sanctions & KYC Non-Compliance Since 2008 Financial Crisis', 27 September 2018.
59. US FFIEC, 'Bank Secrecy Act/Anti-Money Laundering Examination Manual', p. 40.

slowing, remains extremely high by historic standards.[60] One recent estimate suggests that banks alone spend more than $12 billion a year globally, and employ tens of thousands of people on financial crime compliance.[61]

However, this 'insurance approach' also conflicts directly with the FIs' commercial imperatives, which frame compliance as a costly drag on profits. The result is often FI compliance functions zig-zagging between two masters: the regulators; and the business itself.[62] Internal indicators of 'effectiveness' become ones that protect the firm's reputation and its bottom line: the reduction of regulatory fines, the demonstration of 'commitment' by investment in people and platforms, and improving measures of efficiency such as lowering false positive rates, backlogs in alert investigation, and boosting SAR volumes, to name but a few examples.[63] Such concerns were also reflected in a recent UK government report from 2017, which suggested that some UK FIs felt they were being incentivised to focus on 'self-preservation over combatting crime', and to 'divert resources … to satisfy their perception of the supervisor's requirements, even where they believe that these would be likely to yield no tangible prevention of money laundering'.[64]

In the London workshop, several participants suggested that one of the ways to tackle this problem was to augment regulatory exams with more detailed input from LEAs on a range of metrics or variables, such as quality of SARs and FI contributions to financial crime disruption. Others also proposed that FIs should be rewarded for good work in a way that is designed to incentivise them both reputationally and commercially. This might come in the form of public regulatory commendations, offsets against other regulatory fines, or forms of financial relief for investment.[65]

A Fragmented System

Many interviewees and workshop attendees also noted how the fragmentation of the model – between the public and private sector, between agencies, and between private institutions – created multiple frictions which hinder the identification and disruption of potential financial

60. Samantha Regan et al., '2018 Compliance Risk Study: Comply and Demand', Accenture Consulting, 2018; Oliver Bevan et al., 'The Compliance Function at an Inflection Point', McKinsey and Company, January 2019, <https://www.mckinsey.com/business-functions/risk/our-insights/the-compliance-function-at-an-inflection-point>, accessed 10 February 2019.
61. Adrian Murphy et al., 'Efficient and Effective Financial Crime Compliance: Dispelling Three Common Myths to Enable Next Generation Solutions', White Paper, Oliver Wyman, 2018, p. 4.
62. Interview A; Interview B; Interview C; author interview with former senior compliance official, London, 4 March 2019 ('Interview F'); author interview with former senior law enforcement and senior compliance official, London, 18 July 2019 ('Interview G').
63. Interview A; author interview with former senior regulator and senior compliance official, London, 22 February 2019 ('Interview H').
64. HM Government, 'Cutting Red Tape: Review of the UK's Anti-Money Laundering and Counter Financing of Terrorism Regime', 2017, pp. 9–10.
65. Consensus conclusion following group discussion, RUSI Workshop on 'Financial Crime 2.0'.

crime.[66] The growing size and complexity of modern compliance dramatically enhance the possibility of mistakes as the result of stove-piping, duplication, or multiple hand-offs between internal departments and between FIs and outside agencies, examples of which were shared by several interviewees.[67] As disaster expert Sydney Dekker describes, in complex systems, accidents usually emerge because of multiplying relationships and not because of defective components – the more relationships, the greater the risk of accidents.[68]

Under the current model, individual institutions struggle to have a credible view of clients and behaviours. Every FI must collate and protect their own client data for prevention purposes, and despite increasing CDD requirements, it remains difficult for institutions to truly 'know' a customer or understand their behaviours. There is limited scope in most jurisdictions for comparing intelligence with other FIs before issuing a SAR, often leading to confusing duplication when the material arrives at national FIUs. As one interviewee commented, 'many SARs are no more than paperwork that FIs are keeping on each other'.[69]

In comparison, modern money laundering is a relatively fluid 'industry'; the most sophisticated launderers are multinational, multi-banked, using multiple individuals and business vehicles, product types, and typologies.[70] New technology is playing an increasingly important role. For example, the UK's Electronic Payments Association has recently noted how the development of 'bots' has allowed tech-savvy launderers to divert transaction monitoring systems by creating patterns of transactional behaviour with legitimate funds that are then replicated with illegal funds, in order to avoid suspicion or perceived changes in behaviour.[71] Although the public and private sectors seek to keep up with the pace of change, the bureaucratic procedures of both sectors often hinder an agile response.[72]

Recommendations

In light of these findings, the author makes the following recommendations:

66. Interviews B; F; G; author interview with senior compliance official, London, 12 March 2019 ('Interview I'); author interview with former senior compliance official and RegTech principal, London, 14 February 2019 ('Interview J').
67. Interviews A; B; C; F; G; author telephone interview with senior compliance official, 22 February 2019 ('Interview K').
68. Sidney Dekker, *Drift into Failure* (Boca Raton, FL: CRC, 2011), p. 63.
69. Interview G.
70. Interviews D and I; author interview with former senior private sector financial crime investigator, London, 8 February 2019 ('Interview N').
71. 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. 28.
72. Interview J.

Recommendation 1: FATF member governments should create or designate a permanent mechanism for improving the evidence base on the impact, costs and benefits of the current AML framework. Its work should cover:

- Ongoing social scientific research on the mechanics and scale of money laundering, and the extent to which the 40 Recommendations positively impact AML effectiveness.
- A redefinition of 'effectiveness', to include cost/benefits and outcomes, as well as quality of policy implementation.
- A revision of the current FATF data collection methodology to take into account changes in the definition of effectiveness.

Recommendation 2: Regulators and law enforcement should work with FIs to better align inter-institutional incentives on the objective of reducing financial crime, by:

- Focusing regulatory assessments on an FI's 'financial crime performance' and integrating law enforcement perspectives into the overall approach.
- Exploring the possibility of reputational and commercial incentives to reward and recognise innovation and contributions to the campaign against money laundering.

III. Innovation

IN LIGHT OF recent scandals and ongoing concerns about the level of the model's effectiveness, there has been a growing appetite for change within financial services, and the regulatory and law enforcement communities in many jurisdictions. For FIs, self-interest has played a significant role. Many large banks have faced regulatory censure for past compliance failings and are now seeking to leverage opportunities to innovate, win back reputation and manage down compliance costs. In several major banks, this has led to an influx of risk professionals from government, regulation, law enforcement, and intelligence, along with data specialists, who have added a further 'spin' to the motor for change.[73] More impetus has come from the expansion of the FinTech and regulatory technology (RegTech) sectors. Many start-up entrepreneurs (usually with limited backgrounds in compliance) struggle to understand why the AML model is not keeping up with technology, and are seeking to push beyond the standard platform solutions.[74] This chapter explores four key themes in innovation, highlighting those initiatives that appear to be having the greatest positive impact (and potential impact) on the barriers to effectiveness in the financial sector.

Culture and Integration

Culture and structure have been significant problems in many FIs, as highlighted in an advisory from the US Treasury's Financial Crimes Enforcement Network in 2014.[75] Financial crime risk management and compliance functions have typically lacked a prominent, single voice at senior executive levels and have not always been seen as part of an FI's core mission.[76] An early aim for many FIs' post-regulatory action has therefore been to change internal culture, by giving financial crime risk greater prominence. This has led to increased financial crime awareness training and guidance, the appointment of board-level 'financial crime risk directors', and the introduction of non-executive directors to oversee the changes.[77] To underpin this, many large FIs have also pursued integration programmes to reduce vulnerability to 'stove-piping' and

73. Interviews A; B; H.
74. Interview J; author interview with RegTech principal, London, 23 May 2019 ('Interview O').
75. Financial Crimes Enforcement Network (FinCEN), 'Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance', August 2014.
76. Interviews A; H.
77. Interviews A; H; L; author interview with current non-executive director, London, 13 March 2019 ('Interview P').

internal friction. Vertical integration within financial crime-related departments has been most common, with examples of:

- **Unified financial crime functions** including all financial crime risk types, often even the traditionally separate function of fraud.[78]
- **Unified activities** where there are clear similarities between the patterns of work – such as AML, fraud and sanctions-related investigations.[79]
- **Connected decision-making** where elements of compliance have traditionally operated in parallel lanes, such as policy, advisory and operations, and there have been attempts to bring senior decision-makers together in designated cross-disciplinary committees.[80]

FIs have also been seeking to improve lateral integration, with 2LoD functions moving into 1LoD, closer to the front line business. In one example provided by an interviewee, an international bank's commercial banking function has introduced an alert system for low-level unusual account activity that goes directly to relationship managers, who can more swiftly deal with it in the context of knowledge of the customer's business.[81]

Assessment

Anecdotally, the enhanced acculturation of front line business into a financial crime risk mindset appears to be paying dividends in the agility of decision-making. An interviewee from a major European bank noted how the integration of 'volume' tactical financial crime decision-making into 1LoD was opening the opportunity to allow the most difficult matters to be dealt with in conjunction with specialists in 2LoD. Not only does this facilitate a better use of resources – those with deep expert knowledge dealing with the most complex problems – it also reduces many of the multiple handoffs that plague risk-management models under the TLoD.[82]

Vertical integration has proved more challenging. Bringing departments and functions together through merger has slowed operational delivery, at least in the short term, and created cultural clashes between those who have long operated in different spaces – especially AML and fraud.[83] In addition, the reshaping of functions has resulted in the creation of new divisions within an apparently more unified function. Interviews revealed several examples of structural change leading to uncertainties around roles and responsibilities, duplication, 'mission creep', and bureaucratic conflicts, which one interviewee described as a *Game of Thrones*-style environment. Moreover, the process of vertical change, once begun, is hard to stop, as new

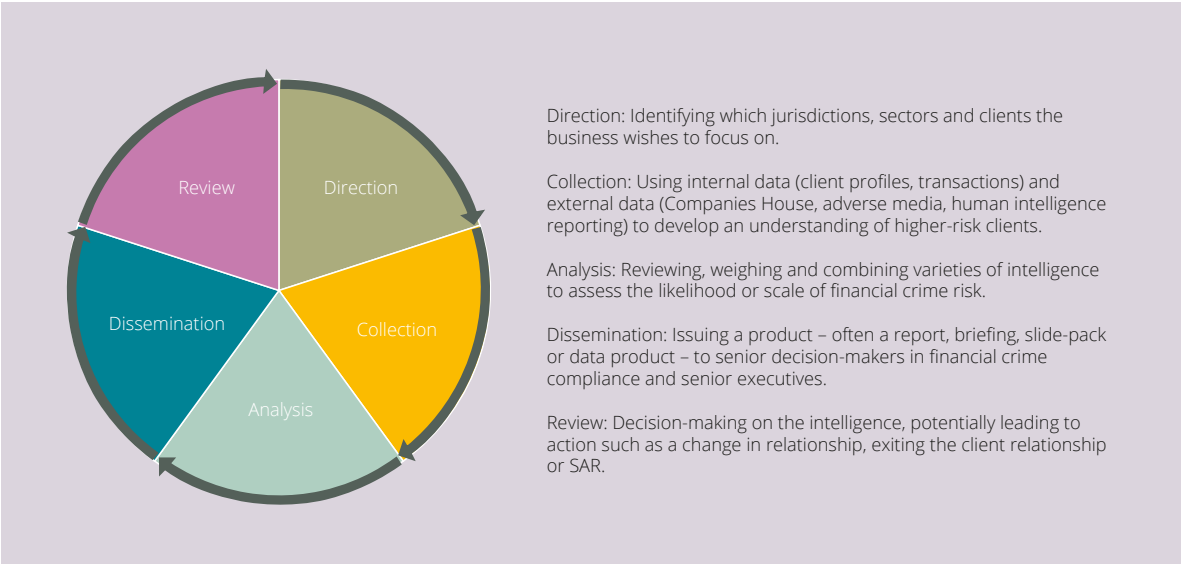
78. See, for example, PwC, 'Building a United Front on Financial Crimes', October 2018.
79. See Regan et al., 'Comply and Demand', p. 6.
80. Interviews A; C; H; P.
81. Interview N.
82. Interview K.
83. Interviews A; B; C; G.

structural changes are introduced to rectify issues from previous changes, fostering fatigue and low morale.[84]

Intelligence

Since the 1980s, FIs have increasingly used political risk-management consultancies to undertake EDD on clients and potential clients, especially in emerging markets. Many firms continue to use such services, but several have also developed in-house intelligence teams to reduce costs and enhance agility. Following the integration trend noted above, several FIs have sought to combine pre-existing intelligence functions into financial crime compliance and risk-management structures.[85] Intelligence teams are called by a number of names, although the term 'financial intelligence unit' is often used. Intelligence teams are typically led and heavily staffed by individuals with government and LEA backgrounds and operate via the core principles of the commonly accepted 'intelligence cycle'.[86]

Figure 3: The Intelligence Cycle



Source: Digital Shadows, 'The Intelligence Cycle: What is it Good For?', 2019, <https://www.digitalshadows.com/blog-and-research/the-intelligence-cycle-what-is-it-good-for/>, accessed 12 April 2019.

84. Interviews C; N; author interview with senior compliance technology specialist, London, 12 March 2019 ('Interview Q').
85. Interviews A; B; D; G; K; L.
86. See Mark Gregory and Tom Salmond, 'A Smarter Way?' *inCOMPLIANCE* (Vol. 18, Winter 2014), pp. 12–15.

Technology also features heavily in FIs' use of intelligence, with data analytic and networking tools often used in the process of collection and analysis.[87]

Assessment

Intelligence-led approaches have helped focus FIs more on underlying risks and 'bad actors' – organised criminals behind human and drug trafficking or cybercrime, corrupt kleptocrats and terrorists – rather than single transactions.[88] The presence of intelligence within the context of commercial financial institutions is not without its challenges, however, and some interviewees questioned whether it had lived up to expectations.[89]

Integrating intelligence findings into day-to-day risk decision-making did not happen if appropriate delivery and decision-making channels were not created in parallel. And even if they were, the introduction of intelligence products had often not been as influential, decisive or welcome as originally hoped.[90] Given that FIs run on profit, every piece of intelligence that might lead to the loss of revenue is open to challenge. One former compliance professional, now a regulator, explained how difficult it was to persuade relationship managers to exit even very risky clients, unless those clients were clearly unremunerative.[91] Risk appetite and thresholds of concern also vary between intelligence professionals and more traditional compliance practitioners within the 2LoD. Whereas intelligence analysts seek to develop a 'rich picture' of a target or sector, traditional AML investigators look for evidence to support the suspicion of money laundering that would justify a SAR. This leads many compliance officials and front line business staff to find intelligence interesting, but often irrelevant and sometimes dangerous. Without a 'smoking gun', officials are often reluctant to see a justification for changing a client relationship. Indeed, some prefer not to know, because of the unintended regulatory dangers of 'putting new risk on the table'.[92] Without regulatory protections for knowing the previously 'unknown unknowns', financial intelligence will not be able to provide the same level of benefit to FIs as it does within national security contexts.

Technology and Data

The application of analytic technology has also burgeoned across financial services and many other sectors in recent years. Increased computing power from distributed cloud computing, combined with vast amounts of data from the increasing digitisation of economies and

87. *Ibid*.
88. RUSI workshop on 'Financial Crime 2.0'.
89. Interviews F; J.
90. Interviews I; K; N; S.
91. Author interview with former compliance official and regulator, London, 9 February 2019 ('Interview R').
92. Interviews A; J.

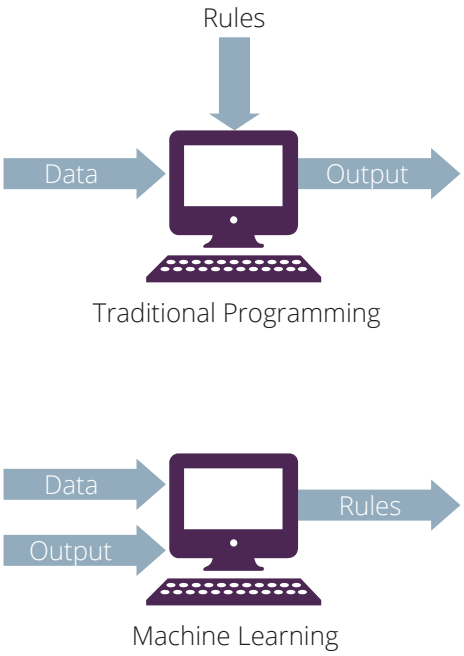
societies, and pre-existing machine learning techniques (see Box 4 and Figure 4), have made industrial-scale data analytics and insight technologically and financially feasible.[93]

Box 4: Machine Learning

Machine learning is a form of AI that relies on mutable algorithms to identify previously unidentified patterns in bulk data. Unlike previous methods of AI, which rely on humans imparting skills and knowledge to computers, machine learning opens up scope for computers to 'learn' through trial and error, rather than human direction. However, machine learning is a wide set of techniques, and levels of required human supervision vary.

Source: Pedro Domingos, The Master Algorithm *(London: Penguin Books, 2015), pp. 1–22.*

Figure 4: Traditional Programming Versus Machine Learning



Source: Guru99, 'Machine Learning Tutorial for Beginners', <https://www.guru99.com/machine-learning-tutorial.htmlhttps:/>, accessed 19 June 2019.

93. See Samantha Regan et al., 'Evolving AML Journey: Leveraging Machine Learning Within Anti-Money Laundering Transaction Monitoring', Accenture Consulting, 2017; Patrick Craig et al., 'Advanced Risks, Advanced Opportunities?', *inCOMPLIANCE* (Vol. 29, 2017), pp. 34–36; Patrick Craig et al., 'Financial Crime 2.0', *inCOMPLIANCE* (Vol. 33, 2018), pp. 25–28.

Institutions are seeking to exploit these opportunities along two tracks, which are not mutually exclusive: first, to improve individual elements of the current model such as transaction monitoring, seeking to make it cheaper and more accurate; and second, to find ways to integrate previously disparate elements of the model, such as CDD systems and transaction monitoring. Interviews with specialists identified three key technologies of most value in these efforts, described in Table 3.

Table 3: Key Technologies for Financial Crime Risk

Natural Language Processing (NLP)	Entity Resolution	Machine Learning Analytics
Value: Collating Data The use of machine learning algorithms has made it possible to translate human communication (spoken, written and gestural) more directly into machine-readable data without the need for laborious translation. This makes it easier to 'trawl' for open-source intelligence, often on the internet, on clients or potential clients.	Value: Integrating Data The use of the Python programming language and machine learning libraries has enabled FIs to deduplicate between multiple datasets, create linkages and standardise registries of clients and client behaviour. This makes it theoretically easier to better 'know your customer'.	Value: Insight from Data The use of mutable algorithms on large datasets has radically improved pattern recognition, providing opportunities to better identify anomalous behaviours.

Sources: Interviews H, J, L, O, and Q and author telephone interview with senior compliance technology specialist, 7 March 2019 ('Interview S'); Kyle Rosetti and Rebecca Bilbro, 'Basics of Entity Resolution with Python and Dedupe', District Data Labs, 3 January 2019, <https://medium.com/district-data-labs/basics-of-entity-resolution-with-python-and-dedupe-bc87440b64d4>, accessed 12 January 2019.

FIs have chiefly applied new technology to two main areas of preventative activity:

- **CDD and KYC**: Here, entity resolution has considerable potential for disambiguating and identifying new and existing clients across multiple data sources. Several FinTechs are also using NLP and machine learning pattern recognition in remote onboarding for the IDV of potential new clients.
- **Customer Screening**: RegTech, providers of sanctions and PEP lists, terrorist watch lists and adverse media screening, is replacing previous rules-based methods with those provided by newer entity resolution approaches (see Table 3).

But the greatest hope for machine learning analytics' potential is to increase the accuracy and speed of detection, reducing the percentage of false positives (and negatives), system and staff costs, and generating fewer but better-quality SARs.

- **Transaction Monitoring**: The application of machine learning techniques to client data, their transactions and financial relationships has the potential to help identify dynamic

clusters and patterns of behaviour that are 'typical' for clients of that type. Set against this, machine learning analytics can identify anomalies and variations in behaviour which might indicate grounds for suspicion. Varieties of machine learning that can be applied to this data go well beyond the capabilities of rule-based screening and monitoring systems.

- **SARs**: Machine learning can be used to triage alerts, categorising them as high-, medium- or low-risk. Depending on an FI's risk appetite, such platforms can both hibernate and close alerts automatically, leaving only the highest risk for human review. NLP also has the potential to help create standardised narratives for SARs, which can then be customised by human analysts.[94]
- **Intelligence**: The use of data analytic networking systems by intelligence teams was mentioned above. Such tools are becoming increasingly sophisticated through the application of entity resolution to better deduplicate between clients and enriched by 'web crawlers' and NLP to collate and analyse open source intelligence from the internet and external databases.

As with organisational structures, some FIs are also seeking to integrate many separate platforms to create a broader view of their clients and reduce duplication of effort. A key development has been the creation of 'data lakes', which bring together internal client profile, transaction and commercial data, such as Companies House material, and sometimes trusted open source material, in one unified 'virtual' location.[95] This data can then be manipulated to meet multiple different perspectives (screening, monitoring and investigations, for example), but with a unified workflow to ensure that all the key stakeholders avoid duplicative or contradictory activities. Such unified platforms also hold out the prospect of active feedback loops, where platforms 'learn' as actions are taken, and new discoveries made.

Assessment

Many large FIs have indicated that they are investing in machine learning-based technology. According to a survey of 59 FIs by the International Institute of Finance (IIF) in 2018, 35% were experimenting with and 34% actively using machine learning techniques, while the remainder had plans to do so in the near future.[96] However, most have been reticent to talk publicly about how well the process of applying new technology has gone, with some exceptions. Last year, Jennifer Calvery, HSBC's Global Head of Financial Crime Risk Management, told a conference that the bank was using a new prototype machine learning platform on transaction monitoring that had shown positive early results. She told Reuters that the platform was 'finding suspected

94. Interviews D; E; author interview with senior law enforcement official, London, 22 May 2019 ('Interview T').
95. Interviews J; Q; S.
96. International Institute of Finance (IIF), 'Machine Learning in Anti-Money Laundering – Summary Report', 2018, p. 2.

criminal activity that had only been identified in the past by humans, not by our own systems … It's a gamechanger'.[97] This was a view shared by several technologically aware interviewees.[98]

Nonetheless, the introduction of these new technologies faces significant practical difficulties. Foremost is a competition for talent in data science. According to a 2018 FI compliance survey by Accenture, three-quarters (76%) of respondents saw a gap between data skills currently available to them in-house, and those they required.[99] Indeed, even if FIs buy 'off the shelf' from RegTechs, the implementation of new platforms can still be a painstaking process. Machine learning is highly dependent on 'good' data for good results, and in conventional banks with ageing legacy systems, there is rarely a 'golden source' of client or transaction data. Both are often incomplete, sitting in multiple servers in different jurisdictions. Such problems mean, therefore, that data remediation and/or transformation is a basic prerequisite before data can be used. In the Accenture survey, one in three (31%) respondents at financial institutions said that data-quality issues were key barriers over the next three years.[100] For institutions that work across borders, moreover, differences in data laws are also prohibitive. As the IIF has indicated, many jurisdictions' data laws inhibit full and effective public information sharing within international financial groups.[101]

Even its advocates admit that machine learning has limitations. Supervised machine learning, with greater human involvement, requires a training model and test data based upon the pre-existing understanding of financial crime typologies. This opens up the possibility that the resulting learning algorithm will be biased towards historic activity and past typologies. Unsupervised learning might be more appropriate for identifying the current unknowns, but the more limited the data, the more dangerous the possibility of an 'over-fit' – what Pedro Domingos describes as having 'too many hypotheses and not enough data to tell them apart'.[102] In such circumstances, the number of false positives – alerts that subsequently turn out to be wrong – are unlikely to be reduced in number.

And when these difficulties are overcome, there is the challenge of explicability. Model validation – the ability to explain the workings of any platform or system with repeatable results – is a key requirement of all financial regulators for stress testing of capital requirements, credit- and risk-management policies and models.[103] These requirements can create difficulties for some types of machine learning-based systems. With supervised machine learning, models

97. Trond Vagen, 'HSBC Set to Launch Cloud Based AML System Next Year, Says Senior Official', *Reuters,* 28 November 2018.
98. Interviews L; Q; and S.
99. Regan et al., 'Comply and Demand', p. 3.
100. *Ibid.*
101. IIF, 'Machine Learning in Anti-Money Laundering – Summary Report', pp. 6–7.
102. Pedro Domingos, *The Master Algorithm* (London: Penguin Books, 2015), p. 73.
103. See US Department of Treasury Office of the Comptroller of the Currency, 'Supervisory Guidance on Model Risk Management', April 2011; FCA, 'IFPRU 4.10 Validation' in *FCA Handbook* (London: The Stationery Office, 2014).

are likely to be easier to understand. For example, a model based on decision tree logic will begin from a basic set of rules previously used by a human analyst. In contrast, unsupervised models which identify anomalous behaviour are more difficult to reduce into an easily explainable and repeatable process, especially when data continues to be augmented. Indeed, the point of using such techniques is that they compress the amount of time humans would take to undertake similar tasks and are therefore considerably more complex.

If FIs are to get the most out of the potential for machine learning, regulators need to support their efforts towards greater flexibility in the process of model validation. This means emulating and expanding the progressive approaches taken by GFIN participants to provide 'safe spaces' (known as 'sandboxes') to encourage nascent technological innovation.[104] The potential of machine learning also behoves regulators to look at a revised approach to model validation, based not on clarity of explanation and repeatability but on trust and verification. This might, for example, involve regular, periodic examinations which compare outcomes based on conventional systems, human-based assessment and machine learning-based models. [105]

Partnerships

Sharing knowledge, intelligence and data is a key enabler in reducing fragmentation in AML and depends on robust inter-institutional relationships. Positively, industry associations have been growing across the financial services sector for some time. The best known, the Wolfsberg Group, was created in 2000 by a group of globally significant banks, who have followed the lead of FATF in setting shared common standards around key AML and CTF issues, including private banking and other high-profile risks.[106]

In some jurisdictions, governments have actively encouraged private sector financial intelligence cooperation through legislation. In the US, for instance, Section 314(b) of the PATRIOT Act allows US FIs to share information with each other in a 'safe harbour' from liability, in order to identify and report AML/CTF risks.[107] This legislation has underpinned major private sector collaborations, such as the original Banks Alliance against human trafficking, initiated by the Thomson Reuters Foundation and Manhattan District Attorney Cyrus Vance Jr in collaboration with several major FIs in 2013. This collaboration has since grown into a larger US Banking Alliance and has been replicated in Europe and Asia.[108] The Netherlands also allows

104. FRS et al., 'Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing'.
105. See Deven R Desai and Joshua A Kroll, 'Trust But Verify: A Guide to Algorithms and the Law', *Harvard Journal of Law & Technology* (Vol. 31, No. 1, 2017); interviews O; S.
106. See Wolfsberg Group, <https://www.wolfsberg-principles.com>, accessed 12 June 2019.
107. FinCEN, 'Section 314(b) Fact Sheet', November 2016; interviews A; H; L.
108. The Thomson Reuters Foundation, 'Thomson Reuters Foundation Launches Resource to Help Financial Institutions Tackle Human Trafficking', 19 July 2018, <https://www.trust.org/i/?id=928ac731-8e74-40db-985a-5e5a4464a86b>, accessed 27 February 2019; The Mekong Club and Thomas Reuters Foundation, 'The Asia Pacific Banks Alliance Against Modern Slavery', January

pre-suspicion sharing of unusual financial activity with the authorities, but only directly with the national FIU.[109]

In other jurisdictions, the focus has moved more towards public–private financial information-sharing partnerships (FISPs).[110] The most notable of these is the Joint Money Laundering Task Force (JMLIT), formed in the UK in 2015, but there have been similar developments in Australia, Canada, Hong Kong and Singapore as well.[111]

Box 5: Financial Information-Sharing Partnership Characteristics

- Provide regularly convened public–private dialogue on financial crime threats.
- Act within the law by making use of available information-sharing legislation.
- Enable, to some degree, private–private sharing of information.
- Address a) sharing of operational intelligence, including the identities of entities of concern, to enhance ongoing investigations, or b) collaborative working to build understanding of threats and risks.

Source: Abbreviated from Nick J Maxwell and David Artingshall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', RUSI Occasional Paper *(October 2017), p. 11.*

In several jurisdictions, there have also been collaborations between the private and public sectors to create a more 'joined up' view of clients through shared CDD, KYC and IDV utilities. In 2010, India's Credit Information Bureau (CIBIL) launched CIBIL Mortgage Check, a nationwide database of mortgage client information designed to limit mortgage fraud.[112] Scandinavian countries have developed a shared electronic identification ('eID') called 'BankID', issued by banks in Norway, Sweden and Finland. The eID can be used to authorise payments and confirm agreements via digital channels, and is now used widely in Sweden and Norway.[113] Several

2019, <https://themekongclub.org/wp-content/uploads/2019/06/The-Asia-Pacific-Banks-Alliance-PDF-2019-No-Password.pdf>, accessed 23 September 2019.

109. See Business.gov.nl, 'Reporting Unusual Transactions', <https://business.gov.nl/regulation/reporting-unusual-transactions/>, accessed 20 August 2019.
110. See Maxwell and Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime'.
111. *Ibid*., pp. 13–21.
112. *Business Standard, '*CIBIL and TransUnion Launch CIBIL Mortgage Check', 21 January 2013, <https://www.business-standard.com/article/companies/cibil-and-transunion-launch-cibil-mortgage-check-110090200169_1.html>, accessed 17 March 2019.
113. EPA, 'Facing Up to Financial Crime', p. 23.

Nordic banks have also begun discussions about the creation of a shared KYC utility, and the authorities in Singapore, Hong Kong, Abu Dhabi and Bahrain have been exploring this option for their jurisdictions.[114]

More radically, there are also initial examples of mechanisms that provide opportunities for improving identification of potential financial crime at an early stage and across institutions. In the UK, for example, Pay.UK, a retail payments authority, has collaborated with Mastercard on the problem of 'money muling'[115] to create a 'Mule Insights Tactical Solution', which enables suspicious payments to be tracked across central clearing systems as they move between payment provider accounts, regardless of financial institution.[116]

Assessment

The consensus view from interviews with both public and private sector professionals was that FISPs are improving FI performance when it comes to detection; for example, SARs generated as a result of leads shared at JMLIT are reportedly of consistently higher value to the National Crime Agency than those which are not.[117] In the RUSI report on FISPs issued in 2017, the authors noted that even at a relatively early stage, such partnerships were making an impact. At that time, JMLIT had led to £7 million of suspected criminal funds being restrained, along with the arrests of 63 individuals suspected of money-laundering offences, and the identification of more than 2,000 suspicious financial accounts previously unknown to law enforcement. In Hong Kong too, the creation of the Fraud and Money Laundering Intelligence Task Force led to the restraint of HKD 1.9 million and the arrest of 65 individuals in its first four months of operation.[118] The experience of JMLIT has also helped shape the progress of SAR reform in the UK, where the government is now looking at the tiering of reports, along with the introduction of new technology, to dedicate resources to the highest priority cases.[119]

---

114. See *Finextra*, 'Nordic Banks Explore Shared KYC Utility', 31 May 2018, <https://www.finextra.com/newsarticle/32178/nordic-banks-explore-shared-kyc-utility>, accessed 12 January 2019; *Finextra,* 'Fenergo to Deploy Blockchain-Based KYC Utility in Bahrain', 1 May 2019, <https://www.finextra.com/newsarticle/33755/fenergo-to-deploy-blockchain-based-kyc-utility-in-bahrain>, accessed 1 June 2019; 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.
115. Money mules are individuals who knowingly or unknowingly allow their accounts to be used for the transfer of criminal funds.
116. EPA, 'Facing up to Financial Crime', pp. 2, 24.
117. Interviews D; E; G; L; T.
118. Maxwell and Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', p. vii.
119. The Law Society, 'Suspicious Activity Reports Reform Programme', 24 April 2018, <https://www.lawsociety.org.uk/news/stories/suspicious-activity-reports-reform-programmes/>, accessed 12 January 2019; interviews D; E; G.

However, these positive effects remain relatively small in scale, with collaboration focusing on a small number of complex and high-end cases. Barriers to expanding these partnerships are a lack of law enforcement 'bandwidth'[120] as well as intertwined legal and technical issues which limit pre-suspicion sharing. As the example of the Netherlands above suggests, increased sharing between the private sector and the authorities is possible; however, for a country with a large volume of SARs already, pre-suspicion sharing with the authorities would need to be done in a way that did not simply add to a backlog. One approach would be to reframe reports of unusual activity as future leads for analysis, rather than immediate triggers for action (unless there is indication of a threat to life), as is often the case in practice already.[121]

A more fruitful way forwards would be to follow the US's lead of providing a legal basis for pre-suspicion sharing between private institutions. However, in many major FATF jurisdictions, current data privacy law might be prohibitive. Under the EU's General Data Protection Regulation (GDPR),[122] for example, the need for 'unambiguous consent' (Article 7), the 'right to be informed' (Article 14) and the 'right to be forgotten' (Article 17) all give grounds to challenge the 'public interest test' (Article 23) which provides possible justification for sharing data without a data subject's consent.[123]

Privacy-enhancing technologies (PETs) might provide part of the answer to such issues; the distributed ledgers of blockchain, along with increasingly sophisticated techniques such as homomorphic encryption, provide the possibility of cross-institutional data analysis of what is effectively anonymised personal data.[124] National regulators have therefore been exploring potential PET 'use cases' for financial crime intelligence sharing. For example, tax authorities in the Netherlands, the UK and Belgium have developed the FCINet project, which uses a technology called 'ma3tch'. When a participating agency wishes to share data, it creates an anonymous filter which is sent to collaborators' databases, without prior request. The receiving agency can check whether the selected filter matches the encrypted data in its own database and can then request additional information through the commonly available channels for mutual legal assistance. Nonetheless, such techniques are still relatively novel, and may yet fall foul of stringent data law requirements; a recent review of FCInet, for example, suggested that it might not be fully compliant with laws that require the separation of 'financial crime' information from 'tax' information.[125]

120. Interviews D; E; G; T.
121. RUSI workshop on 'Financial Crime 2.0'.
122. GDPR was implemented in May 2018.
123. Council of the European Union, 'Regulation (EU) 2016/679 of the European Parliament and of the Council', *Official Journal of the European Union* (L199/1, 27 April 2016).
124. See The Royal Society, *Protecting Privacy in Practice: The Current Use, Development and Limits of Privacy Enhancing Technologies in Data Analysis* (London: The Royal Society, 2019); interviews D; Q; S.
125. W Geelhoed et al., 'FCInet: Legal Context and Data Protection', University of Groeningen, Faculty of Law, 2018, pp. 3–4.

While it is appropriate to encourage pilot projects based on PET, this should not distract from the need for governments to review whether data privacy laws are wholly appropriate for contemporary AML. So many potential future developments in AML are likely to rely on the need to share data that there needs to be clearer, more flexible and internationally consistent guidance on data sharing for detecting and preventing money laundering.[126]

The progress of shared utilities is also relatively slow, as the private sector has tended to wait for government or regulatory action rather than initiate such projects themselves.[127] Even where the public sector takes the lead, utilities are proving to have some practical difficulties. In Singapore, the national regulator, the Monetary Authority of Singapore, has been seeking to develop a shared KYC utility for both retail and business customers. This has proved more feasible for individuals than corporations, where a lack of full transparency over ultimate beneficial owners for shell companies creates gaps in the system.[128] However, although gaps in corporate data could be seen as a deterrent for action, they could equally be a spur to improve further levels of global corporate transparency to help such utilities work better.

Recommendations

Recommendation 3: Regulators should identify and share best practice with peers and the private sector on improving organisational agility in FI financial crime risk management.

Recommendation 4: Regulators and law enforcement should identify and share best practice with peers and the private sector on integrating financial intelligence into FIs' financial crime risk-management structures.

Recommendation 5: Regulators and law enforcement should continue to encourage, protect and evaluate FI technological innovation for detecting financial crime risk at all stages of the client life cycle by:

- Ensuring that positive policy statements and 'sandbox' provisions for testing new technologies translate into practical 'on the ground' regulatory support and engagement.
- Developing more flexible 'trust but verify' model validation standards for machine learning-based systems.

Recommendation 6: Regulators and law enforcement should continue to expand legal and technical frameworks for fostering financial intelligence sharing in and between both the public and private sectors by:

- Reforming SAR processes to reduce volume but increase quality and consistency.

126. Consensus view from technology specialists at RUSI workshop on 'Financial Crime 2.0'.
127. Interview L.
128. Jamie Lee, 'Singapore's Know-Your-Customer Utility Experiment Hits Snag: MAS', *Business Times,* 12 October 2018.

- Extending pre- and post-suspicion intelligence-sharing frameworks across the private and public sectors (a potential additional support to Recommendation 4).
- Exploring the use of privacy-enhancing technologies (PETs) to aid data sharing.
- Exploring unambiguous and internationally consistent 'carve outs' from current data privacy laws and regulations to aid data sharing.
- Exploring the development of shared national (and possibly international) KYC utilities, supported by improving corporate beneficial ownership transparency registers.

IV. Prospects

THE DEVELOPMENTS OUTLINED in the previous chapter provide a broad direction of likely travel for the AML framework in the short to medium term, with increasing cooperation across the sectors supported by the exploitation of new technology. How fast and far this will go will vary, depending on how well governments provide leadership to ensure that the potential benefits are felt across the sector.

Inclusivity

These innovations offer the prospect of FIs reducing their cost and programme effectiveness in AML, with the longer-term expectation that these will feed through to better outcomes in reducing the volume of money laundering. However, under the current regime, the benefits of innovation are likely to be unevenly distributed. Each FI is responsible for its own investment choices, giving a significant advantage to larger FIs with deeper pockets.[129] In the absence of the development of shared utilities, therefore, regulators will need to consider ways to ensure that the benefits of innovation are more broadly spread. This might include mechanisms to encourage cross-sectoral cooperation and knowledge sharing, regardless of FI size and type, as well as potential financial burden-sharing across the sector to ensure minimum standards, whether funded by larger FIs, underwritten by governments or possibly a combination of both. According to several interviewees, many major FIs now see financial crime risk management as a competitive issue in which the capacity to innovate will give them an edge over their rivals.[130] If this remains so, however, the danger is that when these larger institutions effectively reduce potential criminality in their accounts, the criminals will simply move to another smaller FI that has fewer resources. AML would therefore remain a matter of 'passing the parcel of risk', rather than reducing it overall.[131]

Balance

The examples of shared utilities and intelligence sharing also raise the issue of the balance between public and private sector responsibility. Several of the interviewed practitioners argued that the AML framework requires a radical rebalancing to put law enforcement, rather than the private sector, in the operational lead. The role of the private sector would no longer be to act as primary gatekeepers, but to provide financial and client data to law enforcement under legal warrant, as happens now in many countries with intercept data related to national security.[132] Several interviewees noted that such an approach would have benefits for the deployment of

129. Interview B; RUSI workshop on 'Financial Crime 2.0'.
130. Interviews A; H; G; B; P.
131. *Ibid*.
132. Interviews J; Q.

machine learning to fight financial crime, as making a larger pool of data available would likely improve the quality of results.[133]

There are limited and basic examples of this happening already regarding financial intelligence in several jurisdictions. The Australian Transaction Reports and Analysis Centre, the Australian FIU, collects, analyses and disseminates financial intelligence data on cross-border currency transactions, suspicious transactions and large currency transactions, while Canada's Financial Transactions and Reports Analysis Centre has required the reporting of cross-border electronic funds transfers made via SWIFT messages since 2002.[134]

However, these are still a far cry from the destination of a public sector-led framework envisaged by some, and workshop attendees recognised that such changes, if they were ever to occur, would take massive policy shifts to generate the legislation, heavy investment and major organisational change that are needed. To drive such initiatives forwards would also take political will and public support to justify the levels of expenditure and changes to data privacy law they would likely entail.[135] Money laundering, although a consequence of major crimes such as drug dealing, human trafficking and grand corruption, is still largely an empty concept in the minds of the public, who, as psychologists have shown, are more likely to be moved to action by shocking imagery than abstract dangers.[136]

However, it might be possible to gather some of the benefits of this approach without undertaking such radical change. Other 'halfway house' options could be considered, taking the model several steps further in terms of public–private partnership while stopping short of a full rebalancing. These might range from networked joint working between FIs with law enforcement and regulatory supervision, to co-located public–private intelligence 'fusion centres'. As one leading compliance technology expert commented, 'this is an intelligence problem that is eminently solvable with technology. There are multiple ways forward. The private and public sector just need the will to explore them'.[137]

Recommendations

Recommendation 7: Governments, regulators and industry associations should work with FIs to ensure that the benefits of innovation are shared equally across the private sector by:

- Encouraging the formation of cross-sectoral private consortia on financial crime.
- Developing knowledge- and burden-sharing mechanisms to encourage the sharing of good practice across the sector, regardless of FI size or type.

133. Interviews L; O; Q; S.
134. Zarate and Poncy, 'Designing a New Anti-Money Laundering (AML) System', p. 10.
135. Interview H; RUSI workshop on 'Financial Crime 2.0'.
136. Cass R Sunstein, 'Terrorism and Probability Neglect', *Journal of Risk and Uncertainty* (Vol. 26, No. 2–3, 2003), pp. 121–36.
137. Interview Q.

Recommendation 8: In the medium term, governments and regulators should explore the costs and benefits of a more unified approach than the current model, whether under public or private sector leadership, by looking at options such as:

- Public–private financial intelligence-sharing networks using PET.
- Co-located intelligence 'fusion centres' bringing together law enforcement and FI financial crime function resources.

Conclusion

'BUT WHAT DO you mean by effective?' a former senior colleague asked when interviewed for this project.[138] He was not the last, as the question spoke to the fundamental ambiguity about the efficacy of the current AML model.

FATF presently defines effectiveness as a measure of how well its Recommendations are implemented, and this sets the tone for national regulators and individual obligated entities. It does not take in how, or how much, those Recommendations affect the underlying problems they are intended to target: financial and predicate crime. It seems logical to think that they will have some impact, but the degree is open to debate. Estimates from academics range from a 'little' to 'not very much'.[139] These assumptions need to be tested with ongoing consistent evidence-based research.

Recommendation 1: FATF member governments should create or designate a permanent mechanism for improving the evidence base on the impact, costs and benefits of the current AML framework.

Whatever the results of such research, the consensus of those working in different parts of the framework is that the current arrangement is probably not optimal, for two basic reasons that go beyond the oft-quoted explanations of private sector laziness or malfeasance:

- **Incentives**: The aim of the framework should be a shared interest in the reduction of financial crime. Under the current model, this is too easily obscured by regulatory, reputational and commercial incentives.
- **Fragmentation**: The current framework is highly fragmented within and between public and private sector institutions. This allows savvy criminals to exploit the vulnerabilities.

To make the framework as it currently stands work better, the first issue should be addressed promptly.

Recommendation 2: Regulators and law enforcement should work with FIs to better align inter-institutional incentives on the objective of reducing financial crime.

Tackling the fragmentation of the system is a larger issue, and one in which regulators, law enforcement and FIs have been seeking to make improvements in recent years; changes are

138. Interview A.

139. Halliday, Levi and Reuter, 'Can the AML System be Evaluated Without Better Data?'.

being made in good faith and go beyond what one senior interviewee termed the desire to simply 'make stupid cheaper'.[140]

Assessing the impact of these innovations at such an early stage, and in the absence of an agreed benchmark, must be both provisional and tentative. On the one hand, compliance costs appear to remain stubbornly high.[141] Some organisational restructuring at FIs has dampened operational gains and weakened morale, while the introduction of intelligence-based channels into several large FIs has sometimes led to conflict with pre-existing commercial and regulatory imperatives. On the other hand, there are definite indications that such initiatives are aiding agility. The lesson so far seems to be to undertake organisational changes with enough sensitivity to ensure that they do not create more problems than they solve.

Recommendation 3: Regulators should identify and share best practice with peers and the private sector on improving organisational agility in FI financial crime risk management.

Recommendation 4: Regulators and law enforcement should identify and share best practice with peers and the private sector on integrating financial intelligence into FIs' financial crime risk-management structures.

Another promising area of innovation – the use of new technologies such as machine learning to better identify financial crime risk – is currently hampered by regulatory concerns around the sharing of data and pre-existing methods of testing and validation. To explore new technologies' value to the full, regulators should ensure that their strong rhetorical support for innovation translates into effective practical action. Progress in improving the technical and legal basis for data sharing is also essential to secure and extend benefits derived from public–private partnerships aimed at preventing and detecting financial crime risks.

Recommendation 5: Regulators and law enforcement should continue to encourage, protect and evaluate FI technological innovation for detecting financial crime risk at all stages of the client life cycle.

Recommendation 6: Regulators and law enforcement should continue to expand legal and technical frameworks for fostering financial intelligence sharing in and between both the public and private sectors.

Two themes that run throughout this paper are the balance of benefit and responsibility. Within the private sector, larger FIs are better placed financially to take advantage of innovation than smaller firms, although their size and complexity can cause frictions in implementation. To ensure that the benefits of innovation have their fullest impact, mechanisms for sharing and implementing best practice need to be found. As noted at the outset, the current model also

140. Interview H.

141. Regan et al., 'Comply and Demand'; Bevan et al., 'The Compliance Function at an Inflection Point'.

puts a heavy onus on FIs and other obligated sectors to police themselves at their own cost, and indeed, at their own regulatory risk. Some of the more radical approaches mentioned above – national KYC utilities and public–private fusion centres, for example – would potentially change that balance. The degree to which the balance of day-to-day responsibility for preventing and detecting financial crime might shift from one sector to the other is a moot point. However, the AML community needs to consider and evaluate longer-term alternatives while seeking to identify the level of benefits generated from the model as it currently stands.

Recommendation 7: Governments, regulators and industry associations should work with FIs to ensure that the benefits of innovation are shared equally across the private sector.

Recommendation 8: In the medium term, governments and regulators should explore the costs and benefits of a more unified approach than the current model, whether under public or private sector leadership.

About the Author

Matthew Redhead is a writer on issues relating to national security, intelligence and financial crime. In 2018 he became an Associate Fellow at RUSI in the Financial Crime 2.0 programme. He worked as a financial crime risk professional at a major global bank for seven years, and as a financial crime consultant to the FinTech and RegTech sectors. He has also served as a government official at the UK Home Office and Ministry of Defence.