Deloitte.

IIF Institute of International Finance

The effectiveness of financial crime risk management reform and next steps on a global basis

The Institute of International Finance and Deloitte White Paper
November 2021

Contents

Executive summary

Policymakers, law enforcement, regulators and the private sector have all taken important steps to protect the citizens that they serve and the economies in which they operate through significant investment in people, processes, and technology. Despite this, it has continued to be difficult to effectively stem the flow of illicit finance.

In this paper, the Institute of International Finance (IIF) and Deloitte Transactions and Business Analytics LLP ("Deloitte") highlight four areas of focus where continued reform could build on the good work and progress already underway globally to help improve the effectiveness of the anti-financial crime framework: 1. the use of financial intelligence; 2. risk prioritization; 3. technology and innovation; and 4. international cooperation and capacity building.

This paper also highlights important instances of ongoing systemic improvements, how similar efforts can be deployed across jurisdictions, and how policymakers could prioritize international cooperation and coherence. Strong global leadership is vital, as is a continued commitment from all stakeholders to take an empowered, proactive, collaborative and outcome-focused approach to tackling financial crime. Only by working collectively as a coordinated international system can public and private stakeholders truly address, and ultimately prevent, domestic and cross-border financial criminality.

Introduction

The threat posed by criminal incursion into the international financial system is a global problem requiring a coordinated, wide-reaching response and a clear public policy focus. An effective framework for fighting financial crime is essential and more needs to be done at all levels to help identify and stem the flow of illicit finance which supports malignant activities such as terrorism, sexual exploitation, human trafficking, fraud, environmental crime, drug smuggling, and cybercrime. There is also an inherent connection between the integrity of finance and the stability of the financial system – with increasingly complex and international criminal activity being a factor that significantly undermines cross-border financial strength. [1]

In 2019, the IIF and Deloitte UK laid a way forward on mitigating illicit flows through a combination of internationally consistent regulatory reform and an intelligence-led approach to financial crime risk management. [2] The 2019 paper identified seven key enablers to a more effective system through a process which canvassed financial institutions (FIs), policymakers, regulators and law enforcement across Europe, Africa, the Americas, Asia, and the Middle East. Those enablers included a focus on information exchange, public/private cooperation, and systemic reform with an emphasis on achieving better outcomes.

Since then, noteworthy progress has been made around the world across those issues, building on years of good work spearheaded by the Financial Action Task Force (FATF) and the collective efforts of the public and private sectors to improve the way financial crime is identified, mitigated, and ultimately prevented. In order to gauge current perspectives from within the financial services industry and the public sector on that progress and the continued challenge facing the global financial crime risk management regime, the IIF and Deloitte US have combined research with interviews of stakeholders at FIs and public authorities responsible for Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) and the wider financial crime policy and enforcement environment across both developed and emerging markets.

The result of that research process is distilled in this paper and aims to present a global outlook on the current state of financial crime risk management and compliance, as well as an updated view on how to continue to enhance the overall effectiveness of the framework for mitigating the criminal misuse of the financial system. With the impact of the COVID-19 pandemic raising novel challenges in relation to financial crime activity,[3] with new risks emerging (including, notably, the potential for criminal abuse of publicly funded climate finance initiatives and continued public sector investment in pandemic recovery programs), and with numerous financial crime compliance reform efforts across the globe, there is fresh opportunity to explore how to address factors that prevent the optimum means of tackling systemic financial crime issues by leveraging sound practices, and addressing gaps in international coordination.

There are a number of the potential approaches laid out in this paper that are already being considered and/or developed by stakeholders, albeit at varying levels of maturity, and some are still to be considered. This paper could also, therefore, assist in encouraging firms, regulators, policymakers, and law enforcement agencies to accelerate these reforms within their respective implementation programs and to work to align efforts across jurisdictions.

As such, Part 1 of this paper lays out examples of noteworthy reform efforts at the international, regional, and domestic levels. Part 2 provides considerations on how to make further progress in the following key areas, considering these reform efforts:
1. The use of financial intelligence
2. Risk prioritization
3. Technology and innovation
4. International cooperation and capacity building

This paper highlights important instances of systemic improvements that are ongoing, how similar efforts can be deployed across jurisdictions and how policymakers can better prioritize international cooperation and coherence. While it is recognized that the financial crime frameworks in different jurisdictions are at different levels of maturity, the global homogeneity of the drivers, effects and solutions concerning financial crime warrant a sustained, collective focus by the world community to continue to deliver outcomes which stop the criminal misuse of finance and its subsequent damage to society and financial stability.

There is an urgent need for efforts in this policy area. Though reform processes must be carefully considered and should take an appropriate amount of time to ensure any negative consequences are assuaged, the criminal element in international finance moves at a rate which can outpace many well-intentioned policy initiatives. As has been seen during the COVID-19 crisis, speed was key to addressing changing methods and modes of criminal behavior. Likewise, technological developments move quickly. If policymakers do not have a full picture of new developments and the opportunities and the threats they may create, then there is significant risk that policy reform will fall short or only be briefly effective. There needs to be a continued focus on delivering expeditious and dynamic improvements to the global anti-financial crime architecture to mitigate threats in a more efficient manner.

Part 1: The global outlook on financial crime risk management reform

The focus on efforts to improve AML/CFT and the broader financial crime ecosystem have been at the forefront of policymaking for decades. The FATF was established as an inter-governmental organization over thirty years ago and has been the leading body in setting global standards and promoting effective implementation of legal, regulatory, and operational measures for combating money laundering and terrorist financing. Bodies such as MONEYVAL, the Asia-Pacific Group on Money Laundering (APG) and the Eurasian Group support multilateral cooperation and application of the FATF Recommendations.[4] National efforts have combined with the work of the private sector to strengthen domestic rules and ensure international standards are effectively implemented. International collaboration of Financial Intelligence Units (FIUs) through the Egmont Group and law enforcement work through such fora as Interpol and Europol actively engage in efforts which target emerging risks across the globe.[5]

In addition to this sustained, long-term focus, it is important to note that a number of additional efforts are currently underway at the global, regional, and national levels to modernize financial crime risk management frameworks through updates to domestic and multilateral regimes. The drivers of such efforts often come from the collective understanding that effective outcomes need to be guided by fundamental reform through enablers of a better system. These enablers continue to include, among others, enhanced information exchange, public/private cooperation, the use of technology, and the coherent implementation of international standards.

While Part 2 of this paper looks at a way forward to enhancing effectiveness in financial crime risk management through such enablers, the following examples of recent reforms (and/or reforms that are underway), highlight the collective importance of addressing both the fundamental building blocks of risk management and the need to find innovative solutions for tackling financial crime. The opportunities presented herein to coordinate reform efforts and address sound practices across jurisdictions – and through international bodies – are referenced across this paper and should be a priority to potentially avoid fragmented approaches to these issues, which can be exploited by criminal and terrorist financiers.

1. **International standard setting bodies:**
   At the global level, the international standard-setting bodies (e.g., the Basel Committee on Banking Supervision, the Committee on Payments and Market Infrastructures (CPMI), and the FATF continue to set requirements and provide guidance to help drive international consistency in the worldwide anti-financial crime framework.

   During the two-year German presidency of the FATF, the body has prioritized countering money laundering and migrant smuggling, environmental crime, illicit arms trafficking and the financing of ethnically- or racially-motivated terrorism.[6] More broadly, the FATF has set important targets around digital transformation of AML/CFT – including issues around data privacy and data pooling – addressing beneficial ownership transparency, tackling unintended consequences from the FATF standards, and continuing to follow through on, among other things, recommendations and guidance around proliferation of financing risk, virtual asset service providers (VASP) and the application of risk-based supervision. Work on enhancing the effectiveness of implementation of FATF measures continues, and a FATF Global Network assessment process is ongoing, which presents valuable opportunities for improving international coherence in standards. FATF has also increased its focus on ensuring the effectiveness of AML/CFT regimes.

   The Financial Stability Board (FSB), CPMI and the Basel Committee, as well as the FATF, are working on an ambitious

roadmap at the behest of the G20 to enable "faster, cheaper, more transparent, and more inclusive cross-border payment services."[7] As part of the building blocks on how payment system enhancements could be achieved, these bodies are considering issues for applying AML/CFT rules consistently internationally, fostering Know-Your-Customer (KYC) and identity information-sharing and, in conjunction with AML/CFT requirements, reviewing the interaction between data frameworks and data protection. This effort holds promise in not only enhancing cross-border payments but also in addressing structural drivers to de-risking and positively impacting many of the ancillary issues which prevent a fully effective global anti-financial crime framework.

The Basel Committee has also amended its guide Sound management of risks related to money laundering and financing of terrorism, enabling greater interaction, cooperation, and information exchange between AML/CFT and prudential supervisory authorities.[8] This globally consistent guidance can assist in filling gaps in this area, including the mechanisms which facilitate such cooperation in the jurisdictional and international context.

2. **United States:** In the United States (US), there is a growing consensus among regulators, legislators, law enforcement, and industry that compliance with AML/CFT requirements, including the amendments passed after the Bank Secrecy Act (BSA), has evolved into a layered and inefficient system that does not serve the needs of law enforcement. In many instances, this has resulted in regulated FIs spending time on activities that may do little to mitigate the risks associated with financial crime. On September 16, 2020, the Financial Crimes Enforcement Network (FinCEN) signaled the start of a multi-year effort to fundamentally reform the AML/CFT regime in the US through an Advance Notice of Proposed Rulemaking (ANPRM) on AML Program Effectiveness.[9] The ANPRM introduced a proposed definition of AML program effectiveness, the concept of Strategic AML Priorities, and a possible regulatory requirement for risk assessments.

   On January 1, 2021, the AML Act of 2020 (US AMLA) became law, and reinforced and codified a risk-based approach for AML/CFT programs. For instance, the US AMLA required FinCEN to establish national AML/CFT priorities for FIs to incorporate them into their AML/CFT programs, and for regulators and examiners to incorporate into rules, guidance, and examinations. As required by the US AMLA, on June 30, 2021, FinCEN issued the first government-wide national AML/CFT Priorities. The publication of the priorities is a significant step forward in shifting the primary focus of US regulators and FIs concerning AML/CFT programs from maintaining technical compliance to a more risk-based, innovative, and outcomes-oriented approach to help combat financial crime and safeguard national security in the evolving financial environment.

3. **European Union:** The European Union (EU) has launched several initiatives aimed at tackling illicit financial flows. The European Commission's (EC) 2020 AML Action Plan set out six areas of focus including the creation of a single rule book, standardization of AML supervision through the creation of an EU level supervisory body, the development of public/private cooperation and enhanced coordination between FIUs.[10] In 2021, the EC issued a legislative proposal taking forward many of the priorities set out in the Action Plan with a separate consultation on public private partnerships (PPPs) and their role in combatting financial crime across the bloc.[11]

   In addition to its efforts to enhance the financial crime risk management framework at the policy level, the EU has created the European Public Prosecutor's Office, which is charged with tackling complex financial crimes against the EU budget in a more coordinated manner. The EU focus on standardization and supervision is understandable given the differing levels of maturity in financial crime frameworks and approaches across member states. It remains to be seen how policy changes may impact the development of collaborative ways of working between the public and private sectors that is a feature of more mature financial crime frameworks, which is discussed further in this paper.

4. **Singapore:** Financial crime risk management, compliance and enforcement continues to remain a top priority for Singapore. The Monetary Authority of Singapore (MAS) persists with its supervisory efforts around robust execution of financial crime risk management in FIs and in encouraging the use of technology and advanced data analytics.

   The Singapore government is one of the global leaders in passing cryptocurrency regulations to mitigate the money laundering and terrorism financing risks associated with these assets. The MAS passed the Payment Services Act (PS Act) in January 2020, which requires entities that deal in and/or facilitate the exchange of digital payment tokens (DPT) to hold a payment services licence. Such providers of DPT services are required to comply with AML/CFT requirements which include the need to conduct risk assessments, perform Customer Due Diligence (CDD) measures and monitor and report suspicious transactions. Amendments to the PS Act were passed[12] in Parliament in January 2021 to enhance the scope of regulated DPT services, and include custodial services and transfer of DPTs.

   In keeping with the theme of regulating cross-border transactions, the MAS published in June 2021 a consultation paper[13] on AML/CFT requirements applicable to cross-border business arrangements between capital markets intermediaries and their foreign related corporations (FRC), their foreign head offices, or foreign branches, under Singapore's Securities and Futures Act (SFA) and Financial Advisers Act (FAA). Singapore FIs will be provided a transition period of six months to comply

with the requirement to have policies and procedures in place to oversee the conduct of FRC or foreign offices. These include (i) record-keeping – CDD and Transaction Monitoring information must be kept for at least five years; (ii) internal policies are to be updated relating to CDD and Transaction Monitoring; and (iii) provision of CDD/Transaction Monitoring Records upon request.

In October 2021, the MAS announced that it will implement a digital platform and an enabling regulatory framework for FIs to share with one another relevant information on customers and transactions to prevent ML, TF, and proliferation finance (PF). The new digital platform, named COSMIC, for "Collaborative Sharing of ML/TF Information & Cases", will enable FIs to securely share information on customers or transactions where they cross material risk thresholds. It aims to support FIs to identify and disrupt illicit networks and enhance SARs. The information is shared in a structured data format and is designed to integrate with data analytics tools to help FIs collaborate productively and at scale. The sharing creates an enriched data pool of higher risk activities and customers that FIs can use to dynamically assess customer risks and that MAS will use in risk surveillance to detect illicit networks to target for supervisory interventions. In its consultation paper,[14] MAS explained that it will require participant FIs to implement robust measures to safeguard against unauthorized use and disclosure of COSMIC information.

5. **United Kingdom:** The United Kingdom (UK) has continued to drive enhancements to its financial crime framework through the delivery of the Economic Crime Plan. Significant investments are slated, to build FIU capacity and capability, and to bolster the capabilities of the national fraud reporting service, however these investments come against a backdrop of significant increases in SAR volumes and reported frauds.

   Her Majesty's Treasury (HM Treasury) is undertaking two financial crime-related consultations. The first is to make time-sensitive changes to regulations to enhance clarity in certain areas and ensure compliance with international standards. The second is a much broader consultation, seeking stakeholder views on the overall effectiveness of the AML regime, including on the potential value of new concepts such as the introduction of national priorities similar to those set out in the US AMLA, while also assessing whether key elements are operating as intended

   The Home Office is also expected to consult on potential changes to AML and information sharing legislation in 2021. Between both consultations, there are significant opportunities for stakeholders to work collectively to drive effective financial crime reforms in the UK.

6. **Other global examples:** Though this paper highlights above some specific international and jurisdictional examples that encompass major structural change in AML/CFT rules and supervision, there have been developments across other countries and regions which merit significant attention, and which could be replicated in other places or connected more closely across global reform efforts.

   In Australia, the Australian Fintel Alliance continues to bring together increasing numbers of banks, remittance service providers, and gambling operators, as well as law enforcement and security agencies, to share intelligence and develop solutions on preventing and disrupting financial crime. Investments have also been allocated to enhancing reporting systems for FIs to streamline compliance and drive more timely and effective financial intelligence. A parliamentary committee is examining the adequacy and efficacy of the national AML/CFT regime and will report later this year.

   More broadly in the Middle East, North Africa, and Sub-Saharan Africa, there is a continued focus on technical assistance and training through organizations such as Middle East and North Africa Financial Action Task Force (MENAFATF) and on building information sharing capabilities. These include efforts such as the MANSA CDD platform in Africa, which has been established by a partnership of private sector and central banks to provide a single source of primary data required to conduct CDD on African entities in order to alter risk perceptions, address de-risking on the continent, and promote trade in Africa. PPPs are being established or are operating in multiple jurisdictions including, for example, in Hong Kong (the Fraud and Money Laundering Intelligence Taskforce), South Africa (the Anti-Money Laundering Integrated Taskforce), and Canada (Project Protect).

   Several jurisdictions within Europe are also innovating to enhance their response to financial crime beyond the EU-focused reform initiatives noted herein. For instance, in Sweden, five banks and Finanspolisen Rikskriminalpolisen – the Swedish FIU – formed the Swedish Anti-Money Laundering Intelligence Task Force (SAMLIT), which is a co-operation for the sharing of operational information, with work ongoing to include more banks in that effort.

   Other examples include the development of information sharing utility models such as 'Transaction Monitoring Netherlands' [18] and Invidem in the Nordics[19]. The Nordic and Baltic countries have also formed the Nordic-Baltic AML/CFT Working Group, which is designed to allow authorities to exchange experiences and information on financial crime matters across countries and agree on measures to increase cooperation.[20]


100%
90%
80%
70%
60%
50%
40%
30%
20%
10%

Part 2: A way forward on continuing to enhance effectiveness in financial crime risk management

As recognized in Part 1 of this paper, a critical opportunity exists now to make meaningful changes in how the global financial community addresses illicit finance and to build upon the advancements of the past several decades. Momentum for reform is being driven by the collective need to mitigate and prevent financial crime consistently across borders and across industries and sectors. Building on the work that has already been undertaken and efforts which are currently underway, the following areas warrant further discussion and development through public and private sector cooperation and coordination:

1. The use of financial intelligence

The management of financial crime can be improved by facilitating the increased sharing of information, and by more effectively using financial activity, threat and risk data linked to crime and terrorism, both domestically and internationally.[21] Nevertheless, issues such as inconsistent legal frameworks for data protection, the management of SAR type information, privacy and bank secrecy continue to present barriers that inhibit an effective intelligence-led approach to risk management. Building on the enablers identified in the 2019 white paper, several key issues remain vital in developing a better anti-financial crime system and should be considered across reform efforts.

a. Suspicious activity and transaction reporting

Background

The Suspicious Transaction Report (STR)/Suspicious Activity Report (SAR) regime is a cornerstone of the global financial crime risk management framework. However, there are a number of acknowledged challenges to its effective application. Legal frameworks penalize the "failure to report", but do not generally sanction overreporting. This encourages reporting institutions to adopt a defensive reporting posture, which – juxtaposed with a low threshold for "suspicion", and an all-crimes approach – drives up SAR volumes without delivering commensurate gains in reporting quality or improved outcomes – for example, increased prosecutions or asset seizures.

High volumes of low-value reporting (whether that be specific transactional data and/or suspicious activity, depending on the jurisdiction), consumes resources in both the public and private sectors in terms of production and review. Often such resources could be more effectively deployed elsewhere to focus on higher-value activities. It also creates risks that a significant number of innocent parties are reported to, and recorded in, government databases in a manner that sits uncomfortably with the concepts of proportionality and necessity enshrined in most jurisdictions' data privacy laws

These challenges are amplified where feedback, information sharing, and prioritization between the public and private sectors are underdeveloped and do not support or inform the accurate identification of suspicion or the effective application of the risk-based approach and can mean reporting institutions may not know which SARs are of high value to the FIU. They can be exacerbated further in jurisdictions where supervisory

frameworks do not prioritize quality over quantity, and do not allow efforts to be dialed up or down against mutually agreed threats or priorities - or points of integration of funds such as can be set out in "Geographical Targeting Orders".

A further challenge is that any incident of serious crime is often inherently multi-national in nature and has touchpoints across multiple institutions. Against this reality, approaches to data and information sharing (including the sharing of SARs) are often limited by national and organizational borders that can only be bridged through processes and arrangements that operate with far less agility than that exhibited and leveraged by criminal networks.

This challenge is thrown into sharp perspective when viewed through the lens of a major international FI. It is well recognized that such institutions can potentially see a complete network of suspicious activity across their global data, but limitations on international information sharing often prohibit this global view being shared with a single (or group) of national law enforcement bodies.

This challenge persists even where intra-group sharing—which has been very usefully encouraged by the proactive stance taken on Recommendation 18 by the FATF[22] —has been supported by guidance at the national level.[23] As such, it remains the case that group wide sharing is not yet synonymous with group wide filing, and so while all the component parts of a comprehensive intelligence picture may exist in the system, they are rarely – if ever – assembled into a complete understanding, and certainly not at pace.

To overcome these issues, SAR mechanisms should be reformed in practical ways to enable them to become more effective. Taken together, these reforms have the potential to increase the focus and quality of SAR reporting and the overall effectiveness of the financial crime framework. Where progress is noted, global policymakers are encouraged to take similarly proactive steps to work with public and private sector stakeholders to identify opportunities to enhance effectiveness in their own jurisdictions.

Recommendations

First, it is important that governments and FIUs continue to commit sufficient resources (human and technological), to the collective analysis of SARs and STRs, with a specific focus on enhancing the speed, volume, and quality of feedback on threats and typologies provided to suspicious activity reporters. Enhanced and timely feedback should be specific, focused, and actionable, for example identifying common payment patterns of concern that identified by multiple reporters, to help the reporting sector refine the focus of its AML controls, and help the system as a whole prevent, detect, and respond to financial crime more efficiently and effectively.

Second, enhanced SAR analysis by FIUs including efficacy indicators, could form a key input into a national threat assessment process. This SAR analysis should be enriched with insight derived from in-depth law enforcement analysis of key cases and investigations which together could, in time, translate into a set of national financial crime priorities agreed collectively between stakeholders; a concept that has now, for example, been established in the US through the implementation of the US AMLA, and is an idea also being consulted on by HM Treasury in the UK. The implementation of national priorities could have a significant beneficial impact on the effectiveness of the SAR regime, if supported by reforms to the supervisory framework that could enable reporting efforts to be dialed up in areas of focus, and dialed down proportionately in non-priority areas.

The flexibility to enable institutions to dial effort up and down to reflect priorities as part of an increasingly outcome-focused regime is critical, as is a recognition that in focusing effort on priority areas there cannot be a zero-tolerance approach to reporting against low-priority areas. Without such flexibility, the introduction of national priorities could create additional reporting burdens, without reducing the high volumes of low value reporting that are currently a feature of most SAR regimes. The effective implementation of national priorities affects a broad range of financial crime matters and is discussed more widely and in more detail in Section 2. Risk Prioritization.

Third, SAR frameworks rely on information being pushed from reporting entities to the FIU. Where national priorities do not exist and limited information and feedback is shared between the public and private sectors, reporting institutions may not be at all clear what information is of value to law enforcement or the FIU.

Even where reporting entities do have a good understanding of threats and risks, regulatory frameworks and examination approaches mandate an all-crimes approach, thereby providing little latitude for reporters to dial up SAR reporting efforts against areas of importance, and to dial down efforts in areas of less importance.

Where specific and targeted national priorities are not in place, policymakers could reconsider the balance between "push and pull" in the SAR framework. The current, "one size fits all" approach to reporting might be replaced with a streamlined

reporting obligation, in which reporters would only be required to provide high-level "notifications of suspicion" to the FIU, limited to core customer data and a synopsis of the suspicion. Such an approach would be entirely consistent with the risk-based approach. Over time this process could become increasingly or entirely automated (e.g., in SARs relating to structuring or unusual deposits or withdrawals, generated primarily due to automatic detection of such payments).

If data within the "notification of suspicion" was of interest to the FIU or law enforcement (e.g., hitting a flagged investigation), the FIU or law enforcement could request further investigation by the reporting entity. The bulk of a reporter's investigative capability would be held in reserve to support such proactive requests from law enforcement/FIU, ensuring analytical and investigative effort within the regulated sector was focused on developing intelligence on matters of genuine concern or interest to law enforcement. This process would allow national frameworks to retain an all-crimes approach, while minimizing analytical effort invested in low value reporting.

Fourth, nations with a commitment to tackling complex financial crime should consider how a global FI's potentially comprehensive insight into an instance of international financial crime could be shared as a complete SAR analysis in multiple jurisdictions, putting a comprehensive picture in the hands of investigators.

Perfection should not be the enemy of progress in this context. It is fully accepted that achieving global consensus on information sharing cross-border is a hugely complex issue, but that should not deter likeminded nations, or groups of nations (such as the G7 or the "Five Eyes" Intelligence Alliance), from building bilateral or multilateral agreements to share aggregated SAR data relating to their jurisdictions in a single report that is filed simultaneously in multiple FIUs. Further discussion on bilateral and multilateral cooperation is considered in Section 4. International Cooperation and Capacity Building.

Progress in policy discussions around bilateral/multilateral SAR filing should be supported by parallel collaboration on data standards and the development of common SAR templates that would help accelerate data integration and analysis, as well as the possible inclusion of unique identifiers such as digital IDs to identify cross-border activity on persons of interest, without sharing personal data where no activity/corresponding SAR exists.

In addition to avoiding geographical silos, it is also important that organizational structures within FIs – for example between AML, cyber and fraud teams – do not put barriers in place that undermine the development of a comprehensive understanding of criminals and criminal threats that operate across thematic silos. Expediting efforts to enhance data fusion across organizations is a key enabler in the development of a comprehensive global SAR.

b. Beneficial ownership reporting transparency

Background

Transparency of beneficial ownership and the reporting of that data is a critical tool in fighting all forms of illicit finance, from fraud to money laundering and corruption. Transparency of beneficial ownership can also help promote prosperity by building trust and clarity for financial transactions and investment.

Though the concept of beneficial ownership registries is embedded in FATF Recommendation 24 (R.24), there is uneven progress in implementation across the globe. Where it is made available, a common theme is that the data is held and maintained by a public body that lacks the mandate, as well as the necessary financial and human resources, to effectively assure the quality of the data. This issue needs to be addressed through both policy change and investment creating a single source of reliable truth.

Though the FATF is currently consulting with its member jurisdictions and other stakeholders on amendments to R.24[24] and while implementation and enhancement to registries are underway at various speeds across the globe, a few key issues should be addressed to enhance international coherence in the design and operation of beneficial ownership information reporting. Given recent developments such as the data leak around the "Pandora Papers,"[25] it is evident there is a lack of transparency in the international system; countries should \ make reform in this area top priority in line with the commitments of the G20 and other international bodies.

Recommendations

First, FIs should not be primarily relied upon to verify the information in beneficial ownership registries, to act as gatekeepers, or to depend on discrepancy reporting as a means of validation. There should be increased emphasis on requiring the legal entities themselves (including corporate entities and other forms of incorporation such as, among others, trusts and partnerships) to satisfy CDD requirements in a verifiable way, with commensurate penalties for non-compliance.

Second, in order for the registry to be reliable, it is important to be clear in R.24 that the public sector stands by the contextual reference data they provide, ensuring it is a source upon which the regulated sector can rely both practically and legally if the integrity of the verification information is appropriate for effective risk management. The issue of reliance is key in this context, having significant potential to reduce duplicative compliance processes (e.g., CDD, and/or ongoing due diligence) across multiple institutions, potentially releasing significant capacity that could be refocused on higher value activities. FIs should not be expected to ensure the quality of information maintained in a beneficial ownership registry and discrepancy reporting should not be relied upon as a means of validation.

Third, access to beneficial ownership information should be made available first and foremost to those who have a legitimate purpose for needing this information, such as FIUs, regulatory bodies, law enforcement and FIs. Security of information and genuine data privacy/protection concerns are key considerations which should be considered when considering access to registries.[26] This will require coordination with and the cooperation of national agencies responsible for privacy regulation. Based on this, tiered access for legitimate interest by other stakeholders beyond competent authorities and FIs could be considered.

Fourth, it is important that further work is undertaken to ensure that inconsistencies in national approaches to beneficial ownership information accessibility and reporting are mitigated. Operational burdens with little to no risk management value arise when countries implement different requirements that seek to yield the same results. Country coordination on common standards would improve both efficiency and effectiveness in risk mitigation by FIs and would also further protect the global financial system. It will also aid cross-border investigations and network analysis in FIUs if there were common fields/\ standards that enabled the registers to be knitted together.

FATF has a significant opportunity to enhance the effectiveness of jurisdictional beneficial ownership registries by ensuring high standards are in place internationally through R.24 which include a regular review of registries to ensure weak spots are mitigated, including the use of false documentation or inaccurate identities to hide beneficial ownership interests.[27] However, it is also incumbent on countries to act now to identify weak spots and address the issues noted herein.

The UK provides an interesting and positive example in this context. The UK registry – Companies House – has mapped out a clear strategy to transform its remit from that of a passive registry to one where it will be an active participant in the anti-financial crime community. Companies House will build capacity – both human and technological – to engage in the proactive analysis of data to identify and share strategic and tactical intelligence on crime. Critically, Companies House will itself take a degree of responsibility for the identification and verification of beneficial owners.

While organized criminals will indubitably respond to these reforms by seeking new ways to try to undermine the integrity of the system, (e.g., using "mule directors", acting as fronts to hide genuine beneficial owners), these risks can be mitigated by proactive information sharing by Companies House around emerging typologies and risk. As such, these reforms represent a welcome strategic repositioning of the role of the company registry in the anti-financial crime ecosystem putting beneficial ownership at the heart of the collective response to illicit finance in a way that can help substantially to prevent and detect the criminal abuse of company formation. Ambitious reforms like those proposed by Companies House should be monitored and, if successful might be emulated internationally.

c. Data utility models

Background

It is vital that best use is made of the capacity that exists in the global financial crime ecosystem. Financial crime risk management frameworks globally should enable and encourage modernizations that have the potential to minimize low-value activities so that capacity can be more usefully focused on other, mutually agreed, higher-value activities with greater potential to deliver positive outcomes.

Data and information utilities are important in this context, which, for the purposes of this paper, we define as mechanisms that either allow duplicative processes to be undertaken once on behalf of many (e.g., KYC utility), or which allow siloed datasets to be brought together in information sharing utilities (both public-to-private and private-to-private), either through data pooling, or through the use of collaborative analytics, to enhance the efficiency and effectiveness of risk management functions (e.g., a transaction monitoring utility). Digital identity also has significant potential to be an important category of mutualized data (a form of utility), at the heart of financial crime prevention.[28]

Fulfilling KYC obligations might be considered an inefficient process when assessed at the whole-system level. Developing an approach that would allow this process to be undertaken once

on behalf of all stakeholders could release huge volumes of capacity for reinvestment in other activities, such as participation in PPP and investment in enhanced analytics.

A number of jurisdictions have trialed the development of KYC utilities, most notably in the Nordic region, in Africa and in Singapore. Pilots to-date have identified significant complexities around issues such as the agreement of common standards between participants, the availably of "golden data sources" (and to what extent they can be relied on in a regulatory context), information technology, implementation costs, and the rationalization of legal complications around issues such as the processing of personal data.

These challenges have sometimes slowed or stopped progress. However, they are potentially surmountable over time, especially if lessons learned through both successful and unsuccessful pilots are captured and shared widely and, with the encouragement of regulators and policymakers, are used to inform the development of future efforts to build innovative solutions to address this duplicative and resource-intensive element of the financial crime framework.

There have been a number of interesting developments in the field of information sharing utilities since the analysis in 2019. For example:

- In the Netherlands, through Transaction Monitoring Netherlands (TMNL), five major banks are piloting collective transaction monitoring of combined pseudonymized transaction data to identify unusual patterns of cross-bank activity relating to money laundering. The immediate goal is to enhance the effectiveness of the participating banks' efforts against financial crime, with a potential end state being the development of an industry-wide utility performing transaction monitoring activities on behalf of the FIs involved. While TMNL is a private sector-led initiative, the banks have sought active cooperation with stakeholders in the public sector to build the TMNL platform. For example, detailed typological input has also been provided by the Dutch FIU.[29]

- In the UK, the Tribank[30] pilot pooled transactional data from three banks in pseudonymized form. This was successfully combined into a meaningful dataset over which centralized analytics could be applied to reveal suspicious patterns of activity for further review by bank FIUs.

- In Switzerland, a number of major banks are working together to establish a utility for sharing data for AML alert mitigation. The goal is to create a model that includes agreed systematic triggers which, in the future, would allow the banks to share KYC-derived information to drive timely improvements in data quality and the effectiveness of operation models. A legal assessment was

undertaken to agree on the scope of the utility within current regulations and in accordance with existing customer terms and conditions. The initiative has undertaken a proof-of-concept leveraging transactions that previously triggered AML alerts. The proof-of-concept identifies overlaps between clients and alerts across banks to enable the identification of new typologies and enhance the triage of alerts. An expanded multi-bank pilot slated for completion later in 2021 will test scalability and the value of privacy enhancing technologies to facilitate information sharing.

- In Denmark, the Ministries of Industry, Justice and Taxation have launched a project which intends to assess the feasibility and value of establishing a central analytical platform that will enable FIs' transaction data to be enriched with law enforcement intelligence to improve the collective effectiveness of efforts to prevent and detect money laundering, VAT fraud, and other financial crime. The pilot is being developed under the auspices of the Central Bank, considering issues such as data privacy, technical feasibility, and challenges and opportunities within the existing legal framework.

- In Australia, an amending law to the AML/CFT Act and Rules[30], introduces the opportunity for the regulated community to place reliance on KYC obtained from another regulated party. In order to obtain "KYC reliance" on another regulated party, an institution seeking reliance could undertake both initial and ongoing due diligence on the KYC processes of the other regulated party.

Other countries testing information-sharing utilities include Japan and the US. In the US, FIs wishing to explore information-sharing utilities have the distinct advantage over peers in most other jurisdictions in that the information-sharing provisions set out in the USA Patriot Act enable bank-to-bank information-sharing "in the clear" in certain circumstances.[32] Being able to share data unencrypted has the potential to simplify data integration and centralize analysis as well. [33]

As noted in Part 1 of this paper, in Singapore, the MAS recently announced that it is working in "close collaboration with the [Commercial Affairs Department] and a number of major banks, [to implement] a technology enabled platform for participants to share information on customers exhibiting significant risk red flags and warn each other of potential criminal activity".[34] The development of such a utility is highly encouraging for the potential that it offers to amplify Singapore's collective ability to prevent and detect crime by brigading institutional capabilities.

As might be expected, all recent pilots have – to a greater or lesser extent – confirmed the fundamental hypothesis behind information-sharing utilities, which is that it is possible to identify more criminal activity more effectively when data is brought together for analysis. However, the pilots have also revealed very significant challenges that, if not addressed, have the potential to prevent models from scaling up into "business-as-usual" approaches. These include, for example, issues at the organizational level, such as the incompatibility between data standards and IT platforms, that should be tackled before any information-sharing can occur, as well as legal uncertainty around the interplay between concepts such as data privacy and information-sharing, cross border data sharing, tipping off customers regarding SARs filings, and reliance on third-party data (issues which are explored throughout Section 1. The Use of Financial Intelligence). [35]

Despite the inherent challenges encountered in developing utilities, they remain a concept of potentially substantial transformative value to the effectiveness of the anti-financial crime framework, especially when public and private sector insight is brought together to enable utilities to be truly intelligence-led and aligned with the prioritization of threats. As such, investment and innovation should be actively encouraged, and further consideration should be given to these topics across jurisdictions in the following ways.

Recommendations

First, in order to accelerate and support data utility innovation, it is important that policymakers and regulators provide a degree of certainty about the long-term value of investing in new ways of working. Take, for example, a transaction monitoring utility in which four banks participate. In this case, the long-term value to the system of the utility, is an enhanced ability to prevent and detect crime by analyzing transaction data from multiple institutions. The long-term value to FIs is both social (a greater ability to protect their communities and clients) and commercial (the possibility, for example, that in the future if a set of agreed thresholds around detection of suspicion are met, participants could rationalize their four transaction-monitoring capabilities into one).

Both the public and private sectors benefit if the utility is successful; but development risk currently lies only with the private sector, which generally bears the costs of development and delivery as well as – for example – legal risk, without any long-term certainty on how successful delivery might impact future regulatory expectations. Regulators and policymakers should be prepared to consider sharing a degree of risk (for instance by committing to changes in certain legal obligations if the utility meets an agreed-upon set of criteria), thus helping encourage private sector investment in utility models and accelerating the delivery of a more effective financial crime framework overall. [36]

Second, the use of regulatory sandboxes (e.g., the sandbox run by the Financial Conduct Authority (FCA) in the UK) is important in this context. There are already leading examples of information regulators and financial conduct regulators using the sandbox concept to help encourage innovation. When considering information-sharing utilities, however, it will often be the case that participants will come up against issues that are relevant to both types of regulators (and potentially issues relating to the handling of FIU data as well).

As such, it is important that—at a minimum—information and financial crime regulators, supervisors, and examiners work closely together to help create the conditions in which innovation can flourish. They could also consider working together on the development of experimental collaborative sandboxes through which all potential legal and regulatory challenges relating to information-sharing utilities could be considered and addressed comprehensively to help accelerate innovation. For this to be most effective, financial crime regulators themselves may need to invest in appropriate expertise in order to facilitate the acceptance of new innovation.

Third, there should be further exploration on points of aggregation. Many of the challenges around utilities relate to the need to bring together siloed data. However, there are points in the ecosystem where data is already aggregated to various degrees including, for example, the national payments architecture, national settlement systems, and the correspondent payments networks. Stakeholders in the financial crime ecosystem should collaborate to explore ways to test how centralized financial crime analytics could be run across existing points of data aggregation (e.g., a national payments architecture) to identify and disrupt suspicious patterns of activity efficiently and effectively – including patterns that could not be identified by analyzing data within organizational silos.

It is highly encouraging that the use of the payments architecture to tackle crime is noted as an ambition by some policymakers,[38] although the implicit focus is on using the payments architecture to "design out" fraud. This is an entirely laudable aim and an understandable priority, but public and private sector stakeholders should seek to ensure that the potential dividends of investing in centralized analytical capabilities are fully explored in the context of tackling a much wider set of economic crimes, including money laundering, tax evasion, and other predicate offenses.

d. Public-private partnerships

Background

A PPP – a collaboration between FIs, law enforcement, policymakers, and the regulatory community – has become an important and growing component in global financial crime frameworks. A detailed analysis of the rationale behind the establishment of PPPs, and the value they can add was included in the 2019 white paper.

Since the inception of the UK Joint Money Laundering Intelligence Taskforce (JMLIT) in 2014, PPPs to enable the sharing of intelligence and information have been established in over twenty countries across Asia Pacific, the Americas and Europe. In addition, a number of "single issue" PPP initiatives have been established, bringing diverse stakeholders together to improve the response to specific threats such as wildlife trafficking. Meanwhile, Europol's Financial Intelligence Public Private Partnership (EFIPPP) has continued to develop its role as the first multilateral PPP.

The growth in PPP has also been encouraged by the FATF in policy statements and through the Mutual Evaluation process, and there is now broad consensus that by developing frameworks that better enable more intelligence and insight to flow between parties, it is possible to disrupt malign actors more effectively and better prevent criminal misuse of the financial system. Critically PPPs have begun to change the relationship between stakeholders, building frameworks that encourage and enable parties to share as much as possible, rather than as little as is required. However, while global developments in PPP are a fundamentally positive story, opportunities to do more remain.

Recommendations

First, PPP models have evolved differently in different jurisdictions, with the priorities, types of information and intelligence shared, ways of working, and governance and leadership all reflecting the particular circumstances and characteristics of the country in which the PPP has been established.

While PPPs are currently at different points in their development, national and supranational policymakers could encourage PPP models to develop over time in several ways, including:

- From a policy perspective, PPP should be embedded within the financial crime policy architecture at the national level to ensure that insight and input from across the stakeholder community is captured and used to drive development of effective legislation and regulation.
- At the strategic level, PPPs should be used to drive exponential growth in the development and distribution of strategic intelligence products and typologies. This intelligence should be shared at scale to help inform the effective application of the risk-based approach and to drive consequential improvements in prevention, detection, and reporting.
- At the tactical level, PPPs should find ways to share operational intelligence between stakeholders to expedite investigation and drive outcomes. Tactical information-sharing demands robust governance frameworks and clear legal gateways, but it is vital in driving both effective outcomes against priority threats, and in providing the building blocks in the development of good typologies.

Second, PPPs of all kinds have demonstrated their value. They have built trust and collaboration across stakeholder communities and improved the focus and quality of SAR reporting. PPPs have empowered the risk-based approach, provided stakeholders with access to new intelligence and better insights, and helped to deliver positive outcomes efficiently and effectively for all sides. They should no longer be thought of as a policy experiment and should instead be considered a key component of any healthy financial crime framework. As such, it is important that PPPs are appropriately prioritized and resourced within both the public and private sectors.

Third, Policymakers could consider how participation in PPPs can be incentivized through regulatory and supervisory frameworks, with a focus on reduction/detection of economic crime and the provision of highly useful information to law enforcement. While the value of PPP has been recognized by policymakers at both the national and supranational levels, participation by members of the regulated sector is not formally acknowledged within regulatory frameworks. As such, participation remains a voluntary activity undertaken in addition to regulatory obligations.

The absence of regulatory recognition acts as a limiting factor on the amount of time and resources that institutions can invest in PPP, when balanced against meeting wider regulatory obligations. This undermines PPP growth, restricts investment in new ways of working (such as the development of data utilities), and inhibits the ability of PPP to deliver on its full potential. Reforms under way or being considered in both the US and the UK may provide part of the answer.

The US AMLA establishes the concept of national priorities, and a supervisory framework increasingly focused on the production of highly useful information. Simultaneously in the UK, HM Treasury's consultation on the Money Laundering Regulations (MLR) seeks views on the concept of high and low value activities in the system—which one may assume—once agreed, would be supervised against accordingly.

Recognition that participation in a PPP is a 'high value' activity (with commensurate supervisory expectation that focus is moved from areas of low value to areas of high value) could enable regulated institutions to direct increasing amounts of effort and energy toward supporting PPPs in all forms, from development of policy and typologies to operational support and investment in innovation such as the development of bulk data-sharing utilities.

This, alongside continued progress in associated areas of legislative reform (e.g., to introduce national priorities and to enable more information sharing private-to-private, public-to-private and cross-border as discussed more broadly in the previous topics of this section), could begin to enable a significant shift in allocation of resource within the regulated sector from tick box compliance to intelligence-led collaborative activities of high value to the delivery of outcomes across the financial crime framework – including PPP.

Fourth, PPP leaders should consider how they can tailor engagement with members to build a model that finds the right balance between data coverage and agility. As PPPs establish and grow both through the passage of time and the delivery of reforms such as those described above, there will be natural pressure to expand membership. This pressure exists for a range of reasons, including that increasing membership can be used as a proxy measure of success; that growing membership reduces perceptions of unfairness or favoritism; and, simply, that it instinctively seems logical that a greater number of members means more access to intelligence and better insight.

However, growth also brings challenges. A wider membership can increase governance and administration overheads. It can also make obtaining a consensus difficult, which can inhibit innovation, and it can divert focus from core priorities through pressure to ensure a steady flow of cases or typologies that are sufficiently relevant to all. Most fundamentally, growth for growth's sake can impede the development of trust. For example, in the context of tactical information-sharing partnerships, law enforcement may be less willing to share sensitive case data as membership expands.

An effective PPP model could include tiered membership, blending light touch engagement across a broad range of institutions and sectors, with a smaller set of deeper relationships with a number of core members. Membership of the core would need to reflect agreed priorities and could be cross-sector where required (e.g., where scams are a priority threat, engagement with online platform providers would be key to knitting the online and financial networks together). The core would also need to be sufficiently flexible to respond to changes in the market (such as the emergence of virtual assets) but would almost certainly include the relatively small subset of FIs that in most jurisdictions sit across the vast majority of financial information and intelligence in the ecosystem.

Due to their scale, these organizations would likely have a touchpoint in most cases, the capability to conduct high-quality analysis and investigation at pace in support of the partnership, and the capacity to back the development of new and more effective ways of working, such as physical co-location and the development of innovative approaches to bulk data-sharing and collective intelligence-led analytics. By keeping the core at a manageable size, the group would be more agile in its response to threats and development of innovation.

It would be imperative in such a model that insights obtained by a core group working closely together were routinely captured and shared with the wider regulated sector. This would help to manage perceptions of unfairness and inform the effective application of the risk-based approach more widely and enable collective prevention at scale.

Fifth, public and private sector stakeholders should continue to drive efforts to encourage and enable PPPs to collaborate cross border. Similarly, it is important that where single issue PPPs exist, they work closely with national PPPs in order to share insights against potential areas of overlap (e.g., routes and techniques used in trade-based money laundering and environmental crime) and ensure that shared learning is not lost by looking at issues in isolation.

Sixth, PPP participants should explore the development of digital typologies. By combining traditional law enforcement skillsets with participation from technologists, PPPs may be able to move from paper-based typologies to the creation of digital typologies, coded as a set of rules, that could be more easily and quickly ingested into the transaction monitoring systems of a wider range of institutions. This could help to ensure that the biggest collection and detection capability in the financial crime ecosystem (i.e., the transaction monitoring systems at FIs) was better able to more accurately and quickly prevent, detect and report crime.

e. Data protection and security issues

Background

Issues concerning tensions between data protection and information sharing are not new and cut across nearly all areas outlined in this section relating to the use of data and financial intelligence. They also concern other relevant areas of discussion, including issues for risk prioritization in Section 2 and the adoption of new technology in Section 3. Real or perceived friction between data exchange and rules related to data protection, privacy and confidentiality are recognized as potentially restricting or prohibiting information sharing on matters concerning money laundering, terrorist financing and other threats. However, while the protection of customer/personal data and the right to privacy are of unquestioned importance, the upholding of such principles does not exclude sharing information on illicit financial activity in a safe and secure way. Getting this balance right is therefore critical.

To make progress in overcoming such difficulties and to broaden the ability to share valuable information amongst FIs, law enforcement, and regulators on a cross-border basis a few key issues should be considered.

Recommendations

First, the FATF made substantive progress in this area when it adopted revisions to FATF Recommendation 2 (R.2) on national cooperation and coordination. The amendments expanded the Recommendation to include information sharing between competent authorities and emphasized that cooperation should include coordination with the relevant authorities to ensure the compatibility of AML/CFT requirements with Data Protection and Privacy (DPP) secrecy rules and other similar provisions (e.g., data security/localization). [39]

Once enacted jurisdictionally, this change should help to make sure AML/CFT and DPP rules are accordant and should assist in facilitating exchange of information within the private sector and between governments and the private sector. The FATF itself is encouraged to continue to rigorously review national adoption through criteria which reviews efficacy in line with the FATF's overall objectives. The utility of any Recommendation change is only as good as both its practical application in national rulebooks/guidance and its actual, measurable results in line with both the letter and spirit of the revisions.

In this regard, there should be further focus on whether the outcomes of cooperation have led to changes or clarifications in laws/regulations and material growth in gateways to data exchange. This will likely be the ultimate test as to whether the Recommendation actually supports real progress. [40]

Second, there should be a wider, global focus on addressing the real or perceived tensions between data protection laws and information exchange for financial crime matters on a cross-border basis, and in developing a clear mutual understanding between stakeholders. The FATF, for example, has found there is a noted lack of interaction between national and international AML/CFT and DPP authorities. Such lack of coordination and cooperation might also impede the efficacy of R.2, noted above.

Building on the national-level dialogues mandated through R.2, support should be built on a global basis for an AML/CFT/DPP Forum organized through the FATF, which brings together data protection and financial crime authorities across countries to work on ways to facilitate cross-border exchange of information. The outcome of such a process could drive principles that help reconcile differences in approach and develop solutions leading to determinations of equivalence, or in appropriate cases, mutual recognition of laws and regulations aiming to achieve the same purpose of protecting against financial criminality while upholding data protection and security. This may lead to an enhanced, meaningful exchange of financial crime information, not just between governments but also between FIs, between governments and FIs, and within FIs across jurisdictions.
FATF could prioritize this work through its current project related to data pooling, data analytics and data protection.[42] The FATF have taken a vital step through that project in recognizing that AML/CFT and DPP are both significant public interests that serve important objectives, which are neither in opposition nor inherently contradictory.[43] Indeed, they can be complementary, with the greater the targeted intelligence shared, the more precise the reporting can be. This would lead to less intrusion into private sources and less overreporting of non-pertinent information.

The FATF have also recognized that while DPP laws may differ between each jurisdiction, there is a trend toward convergence.[44] This trend could be capitalized upon through a cross-border AML/CFT/DPP Forum that supports the objectives noted herein with outcomes that can be relied upon as an optimum means for enhancing legal gateways.

It is also important to reconcile work at the FATF level on these issues with work underway at the behest of the G20 concerning enhancements to cross-border payments. The G20 building blocks on how payment system improvements could be achieved includes reviewing the interaction between data frameworks and data protection in conjunction with AML/CFT requirements. The building blocks report raises the difficulties that can come from underlying

legal frameworks and the challenges coordinating and securing support for alignment with international rules, standards, and cooperative supervision and oversight arrangements. Addressing these impediments through a global AML/CFT/DPP Forum may help achieve the wider objectives of the G20 through greater alignment and clarity in laws and regulations across borders.

Third, the issues of data protection and financial crime information sharing should not be discussed in siloed conditions. The wider matters of privacy are often considered issues of human rights and should be reflected in the broader dialogue involving the general public whose information is held across FIs and by competent authorities. [45]

As such, it is extremely important for key actors at both the public and private sector levels to engage with civil society in a proactive discourse on the benefits that can be derived from appropriately sharing information on financial crime matters within the context of DPP frameworks. This dialogue should take two forms: first, an assurance that data privacy and data minimization principles will be upheld to the highest degree while achieving the goals of protecting society and financial stability from the effects of financial crime; and second, addressing general concerns that information-sharing could lead to further financial exclusion of segments of society, exacerbating de-risking issues which have been at the forefront of policy discussions for many years.

The second point is particularly important to address in the context of emerging markets, and greater care should be taken in ensuring that the benefits of information sharing are taken into consideration. For instance, it has been noted that improving data sharing on a cross-border basis can actually lead to more targeted risk assessments by FIs, thus helping to deter wholesale reassessment of client coverage based on inadequate information.[46] The Financial Stability Institute (FSI) has emphasized that improved cooperation on information sharing can help to reduce unwarranted de-risking, which would further aid in enhancing financial inclusion.[47]

As noted in Part 1 of this paper, Singapore has taken a highly measured approach to assessing and addressing information-sharing challenges in their jurisdiction, and a focus on the concerns of civil society is very much at the forefront of delivering improvements to the financial crime framework.[48] As policymakers around the world further examine the means of tackling the critical issues concerning DPP and AML/CFT, incorporating civil society into the discussions will help ensure the objectives of all parties are addressed while moving toward effective change for the benefit of society and stability.

2. Risk prioritization

Background

The relative maturity of financial crime frameworks across different jurisdictions will vary, as will levels of trust and confidence between system stakeholders. In jurisdictions that are less mature, the focus of policymakers, regulators and supervisors both domestically and internationally should remain on ensuring the effective implementation of global standards into national AML/CFT frameworks to build a solid foundation for the risk-based approach.

In countries with more mature financial crime frameworks, however, there is a growing consensus that establishing national priorities – which are the money laundering and terrorist financing risks to which a country is exposed – can help shift the primary focus for AML/CFT programs from maintaining technical compliance to a more risk-based, outcomes-oriented approach.[49] As systems change and effectiveness improves across jurisdictions, considerations such as these should naturally follow, and such a shift should be supported at the international level, including through the FATF.

Specifically, a risk-based approach focused on national priorities can assist the public and private sectors with detecting and reporting more meaningful suspicious activity aligned to areas of importance to the national government. Indeed, according to the FATF, countries should "identify, assess and understand the money laundering (ML) and terrorist financing (TF) risks to which they are exposed. Once these risks are properly understood, countries should be able to implement anti-money laundering and counter terrorist financing measures that help mitigate these risks."[50] The publication of the FATF Guidance on Risk-Based Supervision also makes it clear that a risk-based approach is less burdensome on lower risk sectors or activities, which is critical for maintaining or increasing financial inclusion. [51]

In some countries, such as the US, governments have already established official national priorities. For example, the US Department of Treasury's FinCEN recently published national priorities[52] that are composed from longstanding threats (e.g., international terrorism) and emerging threats (e.g., cybercrime) and are supplemented by strategic documents.[53] In a similar spirit, Singapore publishes its National Risk Assessments, and the financial regulator uses its supervisory activities and its PPP to focus FIs on priority risks including driving the use of data analytics to strengthen detection and reporting in these areas.

In order to identify, evaluate, and mitigate risks associated with the national priorities, FIs should consider how they will adjust their risk assessment processes to focus more closely on applicable priorities and more rapidly understand and incorporate new information received from law enforcement and other sources in the future. Incorporating priorities into AML/CFT programs will likely require a greater focus on understanding specific threats related to applicable priorities and how they may intersect with the FI's business activity.

Once an FI understands how it is impacted by risks associated with the national priorities, it will need the flexibility to refocus resources on higher-risk customers and activities consistent with its risk profile. FIs should consider how they will incorporate additional data and intelligence into their AML/CFT programs and controls on an ongoing basis and national authorities will need to help enable FIs to perform data-driven risk assessments. It is likely that most FIs will also need to develop metrics and examples to demonstrate how their AML/CFT programs align to the priorities and the associated value of reporting to law enforcement. It is important that the global standard setters consider how the effectiveness of FIs, FIUs and examinations will be measured in order to determine whether the information produced is highly useful, and how feedback will be shared across the public (e.g., FIUs to FIUs) and private sectors.

Reallocating resources will also need to be addressed. An effective AML/CFT program ensures more attention and resources are directed toward higher-risk customers and activities, consistent with the risk profile of an FI and the risks associated with the priorities. This will require the FI to be more willing and agile in making AML/CFT program changes including the reallocation of resources. When reallocating focus and resources from lower- to higher- value activities, the FI will need to demonstrate how the resulting shifts are producing highly useful information for law enforcement.

To take advantage of this opportunity, FIs should consider adopting a consistent, repeatable, and defensible approach to procedural changes that can be applied across the AML/CFT program and which satisfies examiners and auditors. A change management process with appropriate governance, documentation, and sign off will be key to realigning resources on more value-added activities. For this concept to work, FIs, law enforcement, regulators, and supervisors will need to be aligned on the local government priorities and the definition of effectiveness.

However, there are clear challenges that could inhibit FIs from dialing down low-risk management value activities or lower national priorities and the reallocation of resources. Within some national frameworks, there is a division between the law enforcement authorities setting the priorities and the supervisory authorities responsible for examining a FI's compliance with regulations. Based on current practices, FI's will likely have to demonstrate to their internal auditors and examiners the reasoning behind why they stopped performing activities that they previously included in their policies and procedures, and why their programs remain compliant. Some FIs might be reluctant to stop activities (even ones producing little value, such as halting the review of alerts that do not identify suspicious activity) due to the concern of regulatory critique. Additionally, some FIs might determine that the burden of (and the time spent on) documenting why a particular activity was stopped is too onerous in terms of general resource allocation.

As such, measuring effectiveness and enhancing the supervisory approach, including establishing clear guidance and expectations, will be critical. Although the risk-based, priorities-focused approach is a welcome reform, nothing will actually change until the supervisory and examination approach changes. It is critical that law enforcement, examiners, auditors, and other program evaluators, including FIs themselves, are on the same page in how to measure and evaluate AML/CFT program effectiveness.

Examiners may need to consider shifting from utilizing a "check-the-box" supervisory approach (e.g., checking if the FI followed every step listed in its policies and procedures) to evaluating whether the FI's AML/CFT program is producing highly useful information for law enforcement and is managing and mitigating threats using a risk-based approach. For instance, examiners could assess the overall quality of the FI's policies and procedures instead of checking whether every element within the procedures was met, including elements that produce low-risk management value.

Examiners could also consider assessing the effectiveness of the FI's threat assessment and how effectively the FI integrated the applicable priorities into the FI's AML/CFT program. For instance, examiners could assess how the threat assessment informed adjustments within the AML/CFT program such as whether the FI reallocated resources toward priority areas and how the FI adjusted its KYC and transaction monitoring processes based on outputs from the threat assessment.

In terms of adjustments to KYC processes, examiners could consider evaluating how the FI enhanced its onboarding, risk rating, periodic reviews and offboarding processes based on the level and type of threat exposure (e.g., if there is a high cybercrime exposure, an FI should consider collecting IP addresses and incorporating them during KYC and transaction monitoring reviews as appropriate). In addition, examiners could evaluate how information collected during onboarding (e.g., nature and purpose of the account) is used to mitigate exposure to risks based on the priorities. Also, if fraud is a national priority, examiners could assess how information is shared between the FI's AML and fraud departments if they are separate, distinct departments within the FI.

Examiners may also consider evaluating the types of alerts generated that are aligned with the priorities; how trends from SARs are used to enhance the FI's overall AML/CFT program; the quality of the SARs filed (e.g., whether the report provides law enforcement with sufficient information to assist an investigation); and how feedback from FIUs on SARs is acted upon to enhance future SARs or build on existing networks where a subject is confirmed to be of interest. Additionally, examiners could evaluate the quality of financial crime risk management trainings on the applicable priorities and associated risks to the FI.

As such, in order to effectively incorporate a risk-based, priorities-focused approach into the AML/CFT framework, there should be additional consideration given to the following areas: examiner training, feedback loop/information sharing on the priorities, threat assessments, demonstrating alignment with national priorities, and pilots.

Recommendations

First, it is important that supervisors examine FIs by using a risk-based approach focused on the priorities rather than solely on technical requirements. If a risk-based, priority focused approach is agreed upon by the public and private sectors, examination materials and guidebooks will need to be updated to reflect the new approach, as FIs use these materials to prepare their programs for exams and, most importantly, examiners use these materials during examinations. Additionally, examiners will need to be trained on the updated instructions. [55,56]

In addition to retraining, an examiner secondment program would help ensure that proper examination processes aligned with priorities are followed. By spending time embedded at the national financial intelligence unit or working at an FI, individual examiners would gain an awareness of how the information gleaned from their exams are used in furthering the national priorities.

Second, strengthening the feedback loop and information-sharing on the priorities between the private sector and law enforcement needs to continue to be a focus of national and regional reform efforts. To have an effective AML/CFT framework, it is necessary that regulators, law enforcement, and FIs effectively share information on threats related to the priorities. Typically, the architecture for information-sharing between public and private entities has domestic statutory roots.[57] It is paramount that law enforcement agencies have leeway in prudently exercising the legal authority to share information on threats related to the national priorities or that gateways be developed to do so. This will create a positive feedback loop where private institutions and the public sector, particularly law enforcement, can continuously share guidance on threats and typologies.

Additionally, where the development of a clear understanding of priority threats requires input from non-governmental organizations (NGOs), they should be engaged through established PPP mechanisms to share actionable learnings that could assist FIs with identifying and reporting on activities associated with priority areas. For example, FIs could incorporate human trafficking trends/red flags received from NGOs into their AML/CFT programs (e.g., onboarding procedures, transaction monitoring rules) in order to identify emerging patterns and file reports on human trafficking activity. Again, legal information sharing gateways need to be considered where facilitation of this data exchange is inhibited. However, clear expectations on the impact of the information sharing should be understood by all actors and particularly regulators who may use the information received to identify unexpected gaps in AML/CFT programs.

Third, there needs to be an adjustment of risk assessment processes to focus more on threats associated with the priorities. FIs will need to adjust their traditional risk assessments and incorporate the use of threat assessments to identify and understand the AML/CFT risks associated with the national priorities more readily. Since existing threats will evolve and new threats will emerge, the FI's threat assessment methodology should be agile, straightforward, and structured to quickly incorporate information from law enforcement and other sources instead of mirroring the "enterprise-wide risk assessment which tends to be very long, complex, and focused on data, documentation, and process rather than outcomes."[58]

Based on information provided by law enforcement, NGOs and other FIs, an FI could use a threat assessment to understand the type of predicate offences associated with the priorities; understand the types of money laundering/terrorist financing cases associated with the underlying predicate offenses; to assess how the predicate offenses could occur based on the types of customers, products and services offered by the FI; and to identify the relevance of the country as country of origin/transit/destination of the laundered funds.[59] Additionally, for priorities like cybercrime, corruption and fraud, FIs will need to assess how to leverage additional intelligence and expertise from across the organization to improve the value of their financial crime reporting to law enforcement.

Fourth, there is a need to develop a shared understanding with the public sector on how AML/CFT programs will be evaluated based on the priorities. There are several ways that the day-to-day operations of an FI's financial crime risk management program can use national priorities to help drive a risk-based approach and demonstrate effectiveness. Based on the FI's size, complexity, customer base, and products and services offered, some metrics or examples that could demonstrate effectiveness include: participation in PPPs; the timeliness of responses to law enforcement and relevant

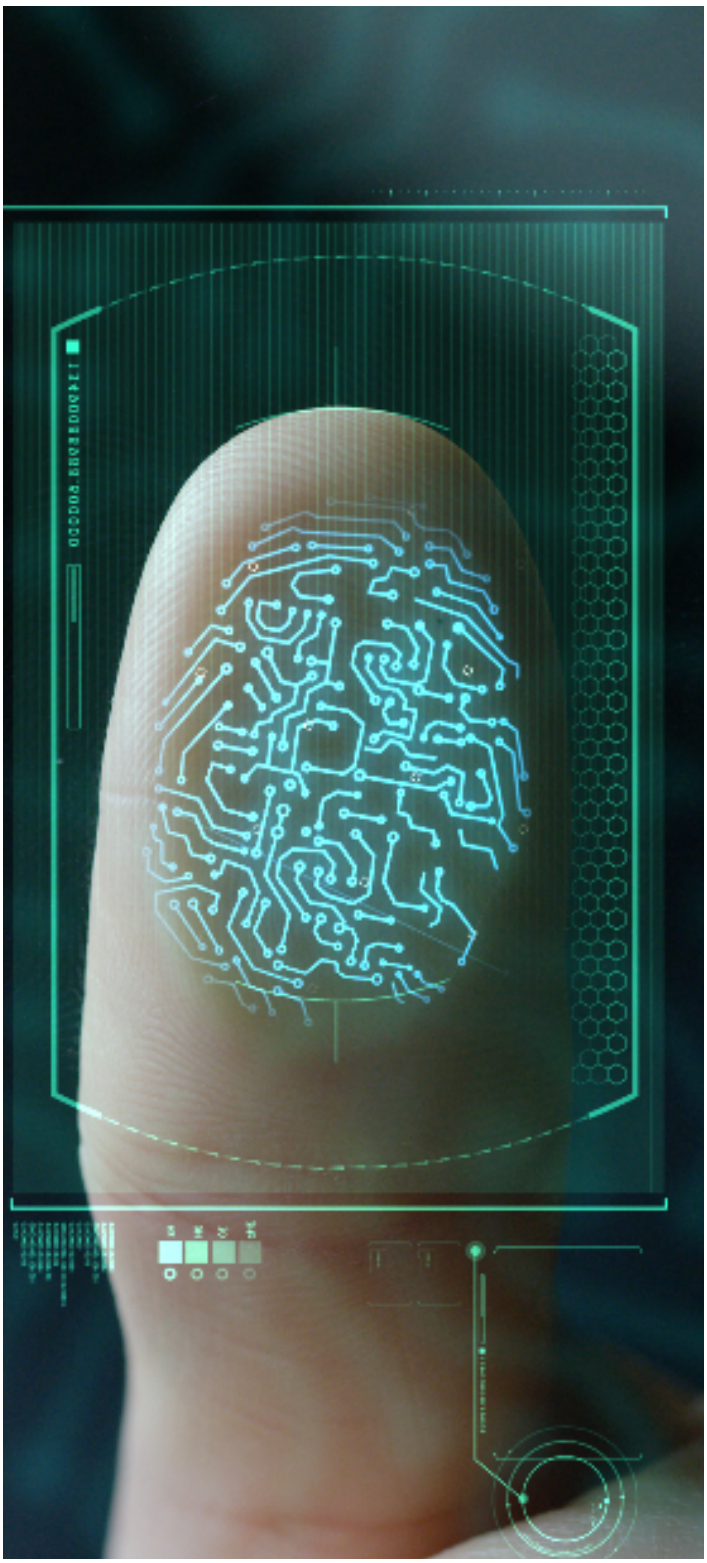
government authorities (e.g., responses to court subpoenas); SARs filed related to the priorities; recognition from law enforcement related to the priority areas; and employee participation in training in applicable priority areas.[60]

Both supervisors and FIs need to calibrate the respective goals of their supervision and AML/CFT programs to produce highly useful information – aligned with the national priorities – for law enforcement. Supervisors could achieve this by providing case studies as examples to demonstrate how an effective AML/CFT program should incorporate the national priorities. One method could be through national FIUs producing domestic-focused case books like the Egmont Group's Best Egmont Case Award for the benefit of all domestic FIs and stakeholders.[61] The cases could be sanitized and aligned with the national priorities, providing FIs with technical assistance, training, information exchange related to leading practices, and developing trends in AML/CFT. These case books can then be shared with the international community through PPPs and international organizations with a level of detail that is helpful to actually accelerate building effective monitoring rules/scenarios to identify activity.

Fifth, there is a need to provide a platform to pilot, evaluate and refine the implementation of priorities into AML/CFT programs. The global AML/CFT community, including supervisors and examiners, should embrace pilots and a regulatory sandbox approach for evaluating potential new risk governance and compliance practices. The development, adoption, and implementation of a risk-based, priority focused approach will take time, and new risk governance and compliance practices should be developed to effectively address the national priorities. A pilot exercise would help facilitate the responsible development of new risk governance and compliance practices by FIs, and new examination approaches and procedures by examiners.

National and local governments could consider developing AML/CFT priority pilots to allow a cross-sector participation of institutions to develop and implement the approaches for incorporating the national priorities into their AML/CFT programs. In doing so, the selected FIs would have an opportunity to reallocate resources and staff to higher-value activities while collaborating with examiners and law enforcement who can provide real-time feedback. By focusing on areas where two or more stakeholders are involved (e.g., FI and examiner, or two FIs for information sharing), the public and private sector can better identify and address barriers that exist between stakeholders.

Throughout the pilot (which is another form of PPP), FIs, law enforcement and regulatory stakeholders should consider participating in a working group to share feedback on the pilot design, examiner evaluation process, and FI effectiveness in addressing national AML/CFT priorities. At the conclusion of the pilot, the working group should publish a report on the lessons learned, provide leading industry practices, and make recommendations for regulatory change.



3. Technology and innovation

Background

The challenges and opportunities inherent in the use of innovative technologies such as machine learning and advanced analytics were considered in the 2019 paper. Since that publication, the use of innovation to improve the overall effectiveness of financial crime risk management programs and disrupt illicit flows in high-risk areas has continued. Progress has been made in some jurisdictions, but also at the international level, in issuing guidance, statements of support, and in some cases passing legislation around emerging technology, with an overall goal of enabling innovation to enhance systemic AML/CFT effectiveness.

The US AML Act, for example, makes innovation and the adoption of innovative approaches a regulatory imperative (e.g., 'NextGen' models that leverage behavioral analytics and machine learning to improve the effectiveness of financial crime monitoring and investigations). Innovation has also been encouraged in a number of countries through the use of regulatory 'sandboxes' that provide a safe space in which new approaches can be tested. The Financial Conduct Authority (FCA) in the UK has gone further, annually hosting a series of Financial Crime Tech Sprints to promote the use of emerging technologies that could combat money laundering and financial crime more effectively.

Innovative information-sharing consortiums have received a degree of regulatory encouragement in Europe, specifically in the Netherlands with the development of an AML transaction monitoring consortium (TMNL), and in the Nordics through the establishment of a Joint KYC utility. In Singapore, the MAS has encouraged and supported the effective adoption of AML/CFT data analytics by FIs. These include solutions that apply machine learning and natural language processing techniques to replicate or enhance operationally intensive processes, such as analyzing name screening hits, priority ranking of transaction alerts for analyst reviews, and network linked analysis to assess higher-risk activities.

Critically, at an international level, the German Presidency of the FATF has prioritized digital transformation in tackling AML/CFT. A coordinated, global focus on advancing technology in this area can help build coherence in approaches across jurisdictions and assist in the development of best practice in driving effectiveness and improving outcomes.

However, challenges remain in the adoption and use of new technologies and it is important that stakeholders continue to work collaboratively to provide clarity on key issues, including for example how the effectiveness of new technologies will be tested and evaluated at the supervisory level.

Recommendations

First, to encourage innovation it is important to clarify how the effectiveness of new approaches will be evaluated by examiners, including how technology can provide improved investigative value to law enforcement.

To achieve this, public and private sector stakeholders need to work together to define investigative value and agree measures and parameters for evaluating effectiveness against it. This would likely require a move away from indicators such as 'the number of SARs filed' and towards, for example, an increasingly qualitative analysis of reports made, their usefulness to law enforcement and their alignment with national priorities. Agreeing on a standard of evaluation of program effectiveness through international fora would help precipitate clear guidance for FIs and would help accelerate the adoption of new technologies more able to identify complex patterns of suspicious behavior more effectively.

Finally, supervisory authorities may need to invest in the expertise and training of examiners to facilitate better understanding and appreciation of new technology-driven approaches so that they can be assessed more effectively.

Second, emerging technologies can help an FI to aggregate and analyze significantly more data than in the past by using, for example, machine learning, AI, analytics tools, and data science. These capabilities will become increasingly important as traditional data (e.g., KYC information), is supplemented with new data generated through, for example, the increased use of online banking, all of which can be enriched through aggregation with contextual information made available through proprietary open-source data providers. By leveraging technology and increasing data volumes, FIs will be better equipped to focus analytical efforts on areas of national priority and will be able to identify new and emerging risks more quickly.

The public and private sectors should work together to establish a framework to allow for greater agility around adjustments to transaction monitoring rules and models. Facilitating the ability of FIs to make changes to their risk coverage models to align to new risks and national priorities is critical to realizing the benefits associated with innovative approaches and emerging technologies.

Third, assessing the role of new technologies in tackling financial crime, consideration should be given toward striking the right balance between rules governing data privacy and protection (DPP), and rules governing AML/CFT. The two frameworks are often characterized as being in tension with each other; DPP rules broadly restricting the sharing of data, and the AML/CFT rules demanding it (at least in relation to suspicion).

As noted elsewhere in this paper, information sharing is a critical enabler in enhancing the effectiveness of all aspects of the fight against financial crime. This applies absolutely in the context of technology, where the development of potentially transformative capabilities and outpacing reforms to the legislative framework. As such, it is vital that stakeholders continue to focus their efforts toward defining and agreeing on the correct balance between DPP and AML/CFT rules at both the domestic and international levels to accelerate and enable appropriate technological innovation.

Privacy enhancing technologies (PETs) – specialist cryptographical capabilities, which allow computations to take place on underlying data, without the data owner necessarily divulging that underlying data – can be part of the solution. However, consideration of the use of PETs should be balanced with discussion on the need for regulatory/legal clarity on information sharing and the use of data to support technological innovation as the ultimate goal.

Fourth, stakeholders should focus on increasing understanding in jurisdictions around the world on how new technologies can contribute to better baseline risk and compliance functions. This would likely include additional efforts by technologists to educate regulators, policymakers, and FIs themselves, and would help ensure that the potential value of new technologies was fully understood, helping to accelerate policy reform to enable their use. The FATF should form part of a core component in technical assistance offered to the public and private sectors on increasing AML/CFT programmatic effectiveness through the use of technology.

4. International cooperation and capacity building

Background

Inconsistencies in the application of AML/CFT measures and broader anti-financial crime matters across jurisdictions continues to impede broader efforts to prevent and mitigate illicit financial flows and impact reforms across all areas referenced in this paper. Rules, along with penalties for non-compliance, that are generally congruous domestically and internationally would make it harder for criminals to engage in regulatory arbitrage, exploiting gaps in financial crime protections in one jurisdiction, and would thus eliminate one of the incentives criminals have to channel their operations through jurisdictions they know are less resilient than others.

Issues likewise remain with regard to the effectiveness of national and regional financial crime risk management regimes when set out against key goals that an effective AML/CFT system should achieve.[62] It is often the case that countries may misinterpret both the letter and the spirit of international standards, distorting how they should be successfully applied across a nation's financial crime risk management architecture and how they should be measured regarding actual outcomes that disrupt the activities of money launders, fraudsters and other malign actors. Achieving uniformity when it comes to measuring success for financial crime risk management also stems from lack of uniformity at the jurisdictional level in capturing outcomes of FATF Mutual Evaluations in national risk assessments.

The fundamentals of AML/CFT and the weaknesses of wider financial crime prevention strategies across certain jurisdictions is the result of having less resources to apply to the rudimentary tenets of a system which delivers on risk management and compliance objectives. The issue of fundamentals also arises in the broader context of understanding between the public and private sectors on the modes of financial intermediation and how best to protect the provision of financial services from criminal incursion.

Progress continues to be made, however, in these areas, as noted in Part 1 of this paper. For instance, the FATF continues its work in measuring effectiveness as part of its Mutual Evaluation Processes, a key component assessing the use and impact of FATF standards and identifying deficiencies in such areas as policy coordination, the application of preventative measures, and approaches to investigation and prosecutions. Through the broader G-20 work on enhancing cross-border payments, the challenges caused by the divergent implementation of AML/CFT requirements is also being examined.
The EU is also currently in the process of revising its standards for AML/CFT regulation and supervision with a focus on consistency in application of rules across the bloc, a push toward more central supervision, and greater cooperation among national authorities and law enforcement. As has been noted, the US is driving toward reforms embedded in the US AMLA which aims to move its system toward a regime focused more on effective outcomes and less on technical or "check the box" compliance.

Nevertheless, there is still a lack of uniformity in progress across the globe around these issues and further work should focus on increased international cooperation and coordination, as well as on building capacity for countries and institutions to get the fundamental building blocks of an effective financial crime risk management framework right. As such, as domestic and international reforms move forward and build on the work currently underway a few key issues should be considered.

Recommendations

First, a continued focus on highly effective implementation of international standards is critical. In addition to the efforts of the FATF on promoting effectiveness in implementation of their

standards, work should progress on how to address improvements to that process. For instance, further risk-based global assessments by the FATF in specific areas should be established, such as the examination by the FATF of all countries at the same time on such issues as information exchange and access to beneficial ownership data. This dynamic approach could potentially remove the lag time between Mutual Evaluations, which can take years and stymie reforms.

Developing common standards regarding the process that countries should follow when implementing FATF recommendations and guidance in order to engage stakeholders appropriately so they can contribute to a better and more coherent regulatory environment overall. Establishing a better process to make implementation of FATF guidance clearer, more effective, measurable, and consistent in FATF member jurisdictions may also help. The strategic review currently underway at the FATF should be used as the driver to address these issues going forward.

More broadly, countries should focus on the basics of what an effective anti-financial crime system means and how that system can be implemented in ways that achieves key objectives. For example, the Wolfsberg Group has stated that supervisors and/or relevant government agencies should assess the effectiveness of FIs AML/CTF programs based on whether they: 1. comply with AML/CTF laws and regulations; 2. provide highly useful information to relevant government agencies in defined priority areas; and 3. establish a reasonable and risk-based set of controls to mitigate the risks of an FI being used to facilitate illicit activity.[63]

Such an approach, if considered collectively across jurisdictions and implemented properly at the supervisory level, will greatly assist in achieving clarity and consistency in regulatory expectations. This will add to the value the private sector can bring to law enforcement and other authorities tasked with delivering on financial crime risk mitigation and prevention measures.

Based on this common understanding on what effectiveness means, even beyond the FATF metrics, should also be considered. There should be more careful consideration given to success in reporting, disruption, and actual arrests and prosecutions to assess whether we are achieving the ultimate goals in the mitigation and prevention of financial crime.

Second, there needs to be greater bilateral and multilateral cooperation globally, focused on delivering specific areas of consistent reform across jurisdictions in an expedited fashion. As such, alongside efforts at global fora like the FATF, FSB, CPMI and BCBS, countries themselves should enhance cross-border dialogue on areas of mutual concern. They should also examine ways to deliver broadly similar outcomes through methods such as equivalence or mutual recognition determinations, memoranda of understanding (MOUs), or enhanced mechanisms of international regulatory and supervisory cooperation.

For example, on-going dialogues across multiple countries currently exist in the area of financial services. These should be leveraged to focus on specific issues where areas of cooperation could be maximized, such as methods of exchanging financial crime information and coordinating interoperability of beneficial ownership registries.

Such cooperation is already taking place in other policy areas. The US and Singapore recently signed an MOU to expand cooperation on cybersecurity, which includes data sharing.[64] Such a process could be replicated across financial crime data and across other jurisdictions. Though the limitations arising from different legal, regulatory, or supervisory regimes are recognized, where comity can be advanced it should be considered a priority of international dialogue and can help address the speed at which reforms can be undertaken. Similarly, the use of supervisory colleges that bring together regulatory authorities across jurisdictions specifically in the areas of AML, CFT and other financial crime matters could be enhanced to focus on areas where MOUs could be developed on key methods of addressing risk in a similar fashion. These dialogues can also provide a better understanding of jurisdictional approaches to financial crime that could be leveraged more broadly, as long as they maximize existing structures and do not add additional layers of complexity or duplication in supervision or compliance.

Enhanced coordination on AML/CFT is also not just an international issue. In national or regional settings there are often myriad actors that play a significant role in government in addressing financial crime. This can lead to inefficiencies and ineffective outcomes. Though there are different approaches how financial crime policy is overseen and enacted across the globe, at a minimum, greater coordination should encompass all facets of the national or regional approach through regulatory, supervisory, and law enforcement cooperation mechanisms—Including through collaboration on prudential measures where needed – and through cooperation with the private sector.

For instance, in the EU, consideration is being given to a central AML authority across the bloc which aims to establish a single integrated system of AML/CFT supervision. Such centralization may not be appropriate in all cases and requires careful design and implementation, but certain principles should be considered more broadly in this area. Specifically, thought should be given to how

countries and regional authorities can encompass greater consistency in hierarchical powers for oversight/enforcement and greater coordination of regulatory/supervisory bodies and FIUs, along with coordination across other countries and with the private sector.

Third, ensuring the fundamentals of financial crime risk management are right is a global priority.[65] Much has been discussed in recent years about building capacity at FIs through training and technical assistance in response to the issues around "de-risking" and, indeed, this has formed part of the work at the FSB's Correspondent Banking Coordination Group in response to trends that contributed to a decline in that type of financial activity.

However, the issues are broader than simply working to address one aspect of financial intermediation. Addressing inadequacies across jurisdictions more generally could assist in achieving further uniform outcomes in cross-border compliance and risk management. Additional work should thus be considered on education, training, and technical assistance across all measurements of effectiveness as defined by the FATF, [66] including for public and private sector stakeholders. Standards implementation can be improved through education programs, training and supporting the FATF. Technical assistance to help governments, regulators, and FIs improve their AML/CFT legal and regulatory frameworks and related supervisory practices, is an important step to reducing financial crime risk. The FSB is placed to take this issue up more broadly, in coordination with the FATF and both national and regional authorities, to advance many of the key objectives outlined here.

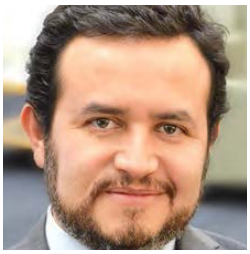
This assistance could take the form of a centralized FSB-led taskforce that could 1. take a stock of current technical assistance programs initiated by the public and private sectors and evaluate their usefulness in achieving objectives aligned with the FATF measurements of effectiveness; 2. based on that exercise, establish principles and practices that can be applied to technical assistance programs globally, while taking account of national and regional specificities; and 3. coordinate amongst governments, international bodies (including the International Monetary Fund and the World Bank) and the private sector on establishing programs where they are required, and enhancing programs where needed, in line with the final principles. Proper public funding to provide countries with technical assistance is also a key factor to consider.

Lastly, capacity building can also be assisted via the cross-pollination of expertise between the public and private sectors. PPPs and other mechanisms for collaboration have worked to enable secondments between FIs and law enforcement or regulatory/supervisory bodies. Capacity building should be encouraged, especially in jurisdictions where it is not a regular facet of interaction between public authorities and obliged entities. At the same time, it will be important to safeguard sensitive information and to clearly demarcate roles.

Contacts

IIF contacts

Tim Adams
President and Chief Executive Officer
+1 202 857 3600



Andres Portilla
Managing Director,
Regulatory Affairs
+1 202 857 3645
aportilla@iif.com

Matthew Ekberg
Senior Policy Advisor,
Regulatory Affairs
+1 202 857-3622
mekberg@iif.com

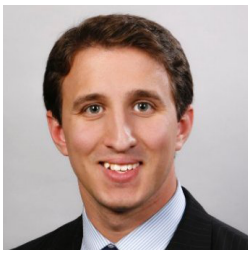
Deloitte contacts

Michael Shepard
Global Financial Crime Leader
Deloitte Global
mshepard@deloitte.com

Clint Stinger
Principal, US AML and Sanctions Leader,
Deloitte Transactions and Business Analytics LLP
Deloitte United States
cstinger@deloitte.com

Chris Bostock
Director, Leader of the Deloitte
Forum for Tackling Illicit Finance
Deloitte United Kingdom
cbostock@deloitte.co.uk

Contributors



Matt Lappas
Manager
Deloitte Risk & Financial Advisory
mlappas@deloitte.com

Yamicha Stephenson
Manager
Deloitte Transactions and Business Analytics LLP
ystephenson@deloitte.com

Endnotes

1. Basel Committee on Banking Supervision (September 2012) 'Core Principles for Effective Banking Supervision' pp. 9 – 14 which refer to the importance of financial integrity to financial stability.
2. For further information on these issues, please see: IIF/Deloitte, The Global Framework for Fighting Financial Crime: Enhancing Effectiveness and Improving Outcomes, October 2019: https://www.iif.com/Publications/ID/3606/The-Global-Framework-for-Fighting-Financial-Crime-Enhancing-Effectiveness-Improving-Outcomes
3. For further information on the impact of the COVID-19 crisis on financial crime, please see: IIF, Staff Paper: Financial crime risk management and the COVID-19 Pandemic: Issues for closer international cooperation and coordination, April 2020: https://www.iif.com/Publications/ID/3867/IIF-Staff-Paper-Financial-Crime-Risk-Management-and-the-COVID-19-Pandemic and FATF, Statement by the FATF President addressing issues concerning COVID-19 and measures to combat illicit financing, April 1, 2020 and FATF, COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses, May 4, 2020
4. FATF, The FATF Recommendations, Updated June 2021
5. FINCEN, GLOBAL WORKSHOP FOR FINANCIAL INVESTIGATORS ON DETECTION, INVESTIGATION, SEIZURE AND CONFISCATION OF CRYPTOCURRENCIES, Updated January 26, 2018
6. FATF, Objectives for the FATF during the German Presidency (2020-2022), June 2020.
7. CPMI, Enhancing cross-border payments: building blocks of a global roadmap, July 2020.
8. BCBS, Sound management of risks related to money laundering and financing of terrorism: revisions to supervisory cooperation, July 2020 and IIF, Re: Introduction of guidelines on interaction and cooperation between prudential and AML/CFT supervision, February 2020: https://www.iif.com/Publications/ID/3752/IIF-Letter-on-BCBS-AMLCFT-and-Prudential-Supervision-Consultation.
9. FinCEN, FinCEN Seeks Comments on Enhancing the Effectiveness of Anti-Money Laundering Programs, September 16, 2020
10. European Commission, COMMUNICATION FROM THE COMMISSION on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing, 7 May 2020.
11. European Commission, Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules, July 2020.
12. "Payment Services (Amendment) Bill" - Second Reading Speech by Mr Ong Ye Kung, Minister for Transport, on behalf of Mr Tharman Shanmugaratnam, Senior Minister and Minister-in-charge of the Monetary Authority of Singapore (4 January 2021), Available at https://www.mas.gov.sg/news/speeches/2021/payment-services-amendment-bill
13. Consultation Paper on Proposed AML Notices for Cross-Border Business Arrangements of Capital Markets Intermediaries under Proposed Exemption Frameworks (12 May 2021), Available at https://www.mas.gov.sg/publications/consultations/2021/cp-on-proposed-aml-notices-for-crossborder-biz-of-cmis-under-proposed-exemption-fwks
14. MAS Consultation Paper on the FI-FI Information Sharing Platform for AML/CFT (1 October 2021) https://www.mas.gov.sg/publications/consultations/2021/fi-fi-information-sharing-platform-for-amlcft
15. The adequacy and efficacy of Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regime, 2021: https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/AUSTRAC
16. Afreximbank: https://www.mansaafrica.com/wps/portal/AFRIXEM_Portal/AboutMANSA/!ut/p/z0/04_Sj9CPykssy0xPLMnMz0vMAfljo8zifSx9DQyN_Q38DMIM3QwczQNCDYMCDI0MPI31g9OK9AuyHRUBBATYRQ!!/
17. Reference and covered in more depth on Page 14 of this paper.
18. Please see: https://www.nvb.nl/english/transaction-monitoring-netherlands-a-unique-step-in-the-fight-against-money-laundering-and-the-financing-of-terrorism/
19. Please see: https://invidem.com/
20. FinCEN, FinCEN Director Emphasizes Importance of Information Sharing Among Financial Institutions, December 10, 2010
21. In November 2017, the FATF adopted revisions concerning the interpretative note to Recommendation 18 clarifying how assessors and advisors should determine the extent of sharing of information at group-wide level, including with branches and subsidiaries, and whether or not sufficient safeguards are in place to ensure confidentiality and prevent tipping-off.
22. This includes countries like UK and Singapore.
23. FATF, Revisions to Recommendation 24 - White Paper for Public Consultation, June 2021
24. The Pandora Papers are 11.9 million leaked documents concerning offshore tax issues and other matters published by International Consortium of Investigative Journalists (ICIJ) beginning on 3 October 2021.
25. Based on this, tiered access for legitimate interest by other stakeholders beyond competent authorities and financial institutions could be considered.
26. IIF, RE: Revisions to Recommendation 24 - White Paper for Public Consultation, August 2021
27. Based on this, tiered access for legitimate interest by other stakeholders beyond competent authorities and financial institutions could be considered.
28. IIF, RE: Revisions to Recommendation 24 - White Paper for Public Consultation, August 2021 Deloitte, Deloitte connects 5 Dutch banks to make an impact with Transaction Monitoring Netherlands (TMNL), 2020
29. FATF, STOCKTAKE ON DATA POOLING, COLLABORATIVE ANALYTICS AND DATA PROTECTION, 2021, Page 11
30. Anti Money Laundering and Counter Terrorism Financing and Other Legislation Amendment Act 2020
31. USA Patriot Act, Section 314(b)
32. Federal Register: Notice of Proposals To Engage in or To Acquire Companies Engaged in Permissible Nonbanking Activities , 314(b) Information Sharing - a Valuable, but Underutilized Tool - RegTech Consulting, LLC
33. Keynote Speech by Ms Loo Siew Yee, Assistant Managing Director (Policy, Payments & Financial Crime), Monetary Authority of Singapore, at the Wealth Management Institute Industry Forum on the Future of Anti-Money Laundering with Artificial Intelligence and Machine Learning on 5 August 2021 (mas.gov.sg)

34. Solutions that are adopted in Singapore to such policy and operational considerations, including data standards, systems connectivity, cross border sharing, safeguards on data protection and appropriate use, are elaborated in MAS public consultation paper at: https://www.mas.gov.sg/publications/consultations/2021/fi-fi-information-sharing-platform-for-amlcft
35. For example, data driven risk assessment as a yearly exercise could be further enhanced by concrete modelling of data already available to local regulators in terms of risk exposure. Such data sets can be made available to regulated entities to enable their respective risk assessments.
36. Please see: FCA, Regulatory Sandbox
37. For further information: Economic Crime Plan, 2019 to 2022 Para 5.8
38. FATF, Outcomes FATF Plenary, 21-23 February 2018.
39. For Recommendation 2, analysis of the FATF Mutual Evaluation Reports (MER) since adoption of the outlined changes reflect action in line with the scope of supervisory cooperation envisioned – with thirty-six jurisdictions assessed under the applicable criteria having a level of compliance in place. However, such an evaluation of compliance does not always fully reflect whether the Recommendation 2 changes have been effective in what we believe should be their ultimate goal – de-conflicting laws and regulations in relation to AML/CFT and data privacy.
40. FATF, Stocktake on Data Pooling, Collaborative Analytics and Data Protection, June 2021, Para 67 IBID
41. IBID
42. IBID, Para 3.
43. IBID, Para 61
44. For example, the right to privacy is a universal human right in accordance with the Universal Declaration of Human Rights and International Covenant on Civil and Political Rights and the implications of this are also reflected in national rulebooks.
45. For example, the CMPI has acknowledged that if banks in a correspondent banking relationship cannot provide additional information on customers and specific transactions due to legal and regulatory restrictions on information exchange, correspondent banks may have no alternative but to block or reject certain transactions. This may in some cases lead to the termination of some banking relationships and contribute to financial exclusion: CPMI, Correspondent Banking, July 2016.
46. FSI, Closing the loop: AML/CFT supervision of correspondent banking, September 2020.
47. MAS is providing legislative safeguards to govern necessary, relevant, and proportionate sharing, appropriate protection and use of information shared and measures to address unintended consequences on customers including potential de-risking.
48. If an FI is a global institution with headquarters in another country that has its own set of national priorities, the local branches of the FI should apply to local accounts the Priorities set by the local country where the branch is based. Local examiners will examine the branches based on the local government Priorities.
49. Financial Action Task Force (FATF), "Money laundering and terrorist financing risks," accessed August 17, 2021
50. FATF, Guidance on Risk-Based Supervision, March 2021
51. Financial Crimes Enforcement Network, "FinCEN Issues First National AML/CFT Priorities and Accompanying Statements,"
52. Such as the Department of the Treasury's 2020 Illicit Finance Strategy, 2018 National Risk Assessment and various FinCEN Advisories. Starting from priorities instead of risks specific to the FI, FIs can align their AML/CFT programs and resources to identify and mitigate risks of primary concern to the local government.
53. MAS' COSMIC digital platform has prioritized three risk areas, namely misuse of shell and front companies, trade-based money laundering and sanctions evasion, in its initial phase of implementation.
54. The US AML Act emphasized the imperative for AML examiners to be retrained. As a result, the requirement for examiner retraining was codified in the new legislation. Section 6307 of the AML Act states that each Federal examiner reviewing compliance with the Bank Secrecy Act (BSA) shall attend appropriate annual training, as determined by the Secretary of the Treasury, relating to AML/CFT activities including with respect to: 1) potential risk profiles and warning signs that an examiner may encounter during examinations; 2) financial crime patterns and trends; 3) the high-level context for why AML/CFT programs are necessary for law enforcement agencies and other national security agencies and what risks those programs seek to mitigate; and 4) de-risking and the effect of de-risking on the provision of financial services.
55. FATF, Guidance on Risk-Based Supervision, March 2021.
56. Such as the Section 314 authority granted by the USA PATRIOT Act or Section 7 of the Crime and Courts Act for the UK's Joint Money Laundering Intelligence Taskforce (JMLIT).
57. The Wolfsberg Group, "Statement on Demonstrating Effectiveness"
58. European Commission, Methodology for identifying high-risk third countries under Directive (EU) 2015/849 and World Bank Group, National Risk Assessment Tool Guidance Manual.
59. Egmont Group, "2011-2013, The Best Egmont Case Award Publication,"
60. Please see: FATF: An effective system to combat money laundering and terrorist financing: https://www.fatf-gafi.org/publications/mutualevaluations/documents/effectiveness.html
61. The Wolfsberg Group, "Statement on Demonstrating Effectiveness"
62. Media Release by MAS, "The United States Department of the Treasury and Monetary Authority of Singapore Finalise a Memorandum of Understanding on Cybersecurity Cooperation" (23 August 2021), Available at https://www.mas.gov.sg/news/media-releases/2021/us-treasury-and-mas-finalise-a-memorandum-of-understanding-on-cybersecurity-cooperation
63. ACFCS, In FinCEN release of AML priorities, Wolfsberg metrics of effectiveness, a glimpse of the future of financial crime compliance, July 202
64. Please see: FATF: An effective system to combat money laundering and terrorist financing: https://www.fatf-gafi.org/publications/mutualevaluations/documents/effectiveness.html
65. ACFCS, In FinCEN release of AML priorities, Wolfsberg metrics of effectiveness, a glimpse of the future of financial crime compliance, July 202
66. Please see: FATF: An effective system to combat money laundering and terrorist financing: https://www.fatf-gafi.org/publications/mutualevaluations/documents/effectiveness.html

Deloitte.

Designed by Core Creastive Services #RITM0862158