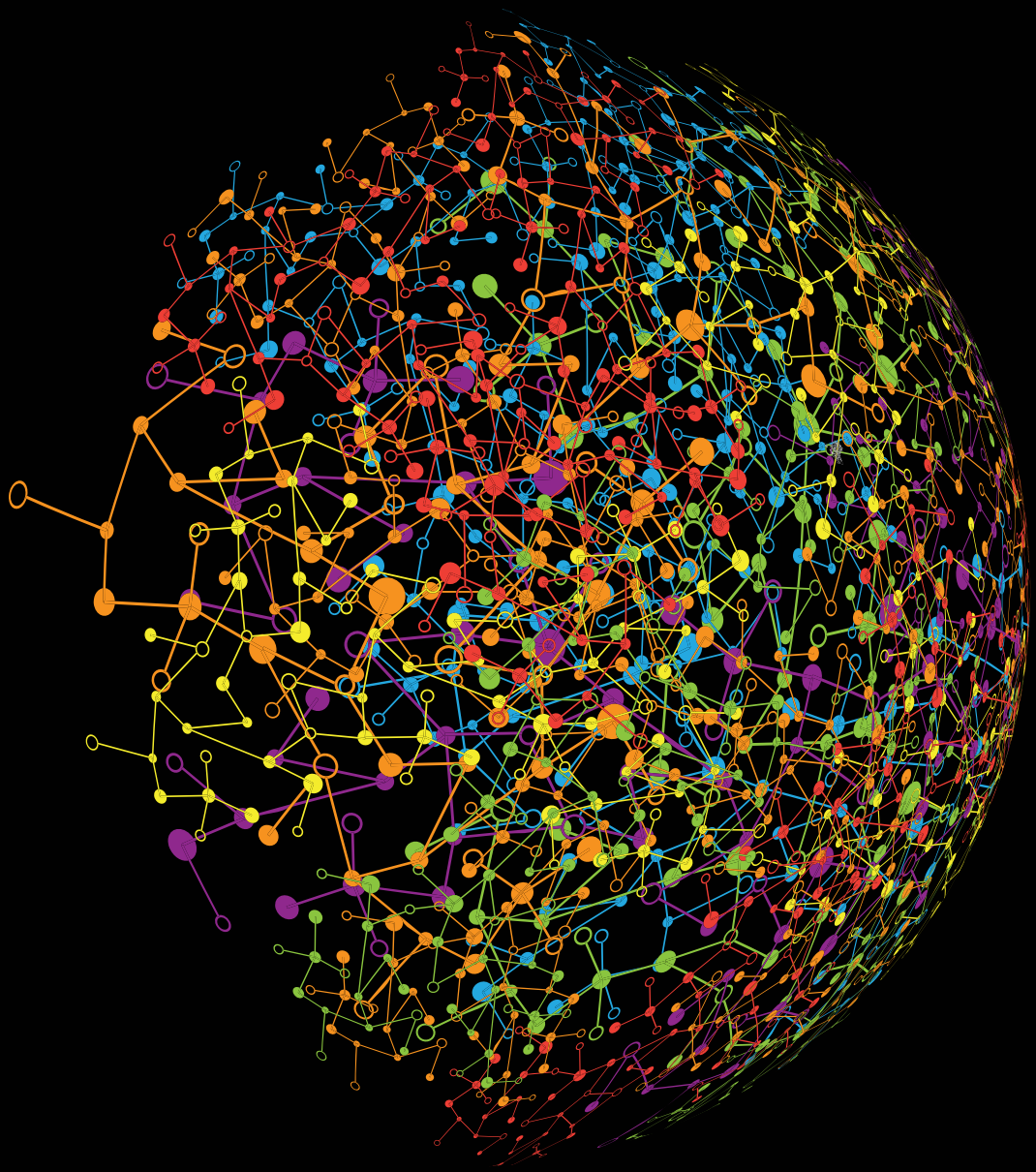
Deloitte.

IIF Institute of International Finance



The global framework for fighting financial crime

Enhancing effectiveness & improving outcomes

The Institute of International Finance and Deloitte LLP White Paper

Contents

Executive summary

There is growing consensus that the current global framework for fighting financial crime is not as effective as it could be, and that more needs to be done at the international, regional and national levels to help identify and stem the flow of illicit finance – an activity which supports some of the worst problems confronting society today, including terrorism, sexual exploitation, modern slavery, wildlife poaching and drug smuggling.

Financial crime is both a contributor to societal ill and a threat to financial stability and financial inclusion, and its mitigation and prevention must be prioritised. While billions have been invested to tackle this type of criminality, greater emphasis needs to be placed on bolstering the efforts of law enforcement with the help of the private sector and ensuring the legal and regulatory framework and financial crime risk management toolkit are enhanced to enable stakeholders to achieve more effective outcomes.

This is not to say that progress has not been made in this area. The Financial Action Task Force (FATF), now in it's thirtieth year, has led the way in internationally coordinated action to reduce cross-border financial criminality and continues to do so in new and dynamic areas. However, a combination of regulatory reform, cultural change, the introduction of new ways of working and the deployment of new technology could significantly enhance the work of governments, law enforcement and the financial services industry in tackling the threats posed on a global basis.

This paper sets out three broad areas of focus for both the public and private sector to consider; the systemic stability and societal effects of financial crime, limitations on the effectiveness of the global financial crime risk management framework and a way forward on improving that global framework.

These are based around seven 'enablers', where reforms of a systemic or tactical nature would enhance overarching effectiveness and would allow incremental improvement at pace, in order to continue the global dialogue on meaningful change. Some are already under consideration or being acted upon through the FATF or in certain domestic or regional circumstances and some represent a new way forward, however, when taken together globally, these have the power to transform how society combats financial crime.

i. Global systemic improvements for financial crime risk management

The effective and coherent application of global standards is one of the primary means by which the financial system can be safeguarded, and criminals can be thwarted in their attempts to profit from their crimes. Inconsistent application of standards can lead to conflict between rules and a breakdown in cooperation which contributes to inefficiencies, negative outcomes and the creation of loopholes that can be exploited by financial criminals.

Factors such as reviewing the threats to financial stability from the fragmentation of rules globally, reviewing and improving the effectiveness of implementation of the FATF standards and guidance and increasing financial, logistical and structural support for domestic and multilateral Anti Money Laundering (AML) and Countering the Financing of Terrorism (CFT) organisations will assist in correcting imbalances which may give rise to systemic concerns on a global basis.

ii. Advancing public private partnership

The Public-Private Partnership (PPP) – a collaboration between financial institutions (FI), law enforcement, policy makers and the regulatory community to tackle financial crime – is central to the effective development of an intelligence-led financial crime model. The development of PPPs is predicated on the recognition that there is a clear overlap between the interests of all stakeholders in fighting financial crime, and that by developing frameworks that better enable more intelligence and insight to flow between parties, it is possible to more effectively disrupt malign actors and better prevent further criminal incursions into the financial system.

While excellent progress has been made in the development of PPP in a number of jurisdictions, there is still work to do in order to fully realise their potential. This paper proposes a number of recommendations to expedite the further development of PPPs, including ensuring that PPPs are supported with appropriate resources, are empowered by enhanced and more effective information sharing gateways, are bolstered with improved technology and are able to work more effectively cross-sector and cross-border.

PPPs present a unique opportunity to help ensure that the right information and intelligence is available to those within the financial crime compliance framework who are most able to use it to drive better outcomes. Regulators and policymakers have a vital role to play in the development of PPPs. Regulatory clarity regarding the role of the PPP can encourage participation and help to increase the overall effectiveness of the regulatory framework.

iii. Improving cross-border and domestic information sharing

The management of financial crime risk can be improved by facilitating increased financial crime information sharing, both domestically and internationally. Such exchange is important to the proper functioning of AML/CFT and other financial crime prevention policies and is also critical in addressing geopolitical priorities such as the prevention of proliferation finance. Yet issues such as inconsistent legal frameworks for data protection, management of Suspicious Activity Report (SAR) type information, privacy, and bank secrecy can present barriers that inhibit information sharing.

At the international level, the FATF are encouraged to continue to drive globally coordinated reform designed to improve effectiveness of its member states' information sharing regimes. Specifically, work should continue to enable information sharing; domestically and internationally at the financial institution group-wide level, financial institution-to-financial institution, financial institution-to-government and government-to-government (in both directions). Implementation of the current FATF framework for increasing the exchange of information should be expedited by the FATF member states and further changes to the FATF standards should be considered to ensure maximum international coherence and effectiveness.

This paper also recommends that governments of the G20 and beyond – and international policymaking bodies – look at early opportunities to encourage greater facilitation of strategic level information sharing, particular typologies and geographic indicators of financial crime risk at the national, regional and international level through PPPs and other mechanisms.

Nations with a commitment to tackling complex financial crime should consider how better use may be made of a global financial institution's potentially comprehensive insight into an instance of cross-border financial crime. It would be beneficial to ensure that where a relatively complete understanding of flows has been compiled, it does not then have to be disaggregated at the point of reporting. Progress could be made in this regard through, for example, the introduction of a 'multinational' SAR.

iv. Improving the use and quality of data

The use of data can be transformative. There is a degree of consensus around the importance and benefits of collating, standardising and making available contextual datasets through utilities that support a consistent process, which can be used by financial institutions to fulfil key Know Your Customer (KYC) and Customer Due Diligence (CDD) requirements, alongside other proactive investigative approaches.

At present, the KYC data landscape is fragmented. Different financial institutions each may hold information on the same customer which may overlap, but which may also be inconsistent and incomplete, a weakness which criminals can navigate in order to exploit the financial system.

Where it is not already possible, extending the availability of centralised corporate information through beneficial ownership registries beyond law enforcement authorities to the regulated sector more widely would enable it to become a force-multiplier in what is considered to be one of the most challenging areas of the KYC process. The continued development of KYC utilities could further reduce gaps in knowledge between financial institutions that can be exploited by criminals while the potential value of digital identification (ID), at the individual and the corporate level as both a means for improving the efficiency and effectiveness of the KYC and CDD process is significant.

It is also important that organisational structures – for example between AML, Cyber and Fraud teams – do not put barriers in place that undermine data sharing and the development of a comprehensive understanding of criminals, and criminal threats, that operate across thematic silos. Expediting efforts to enhance data fusion across organisations is a key enabler of an effective and efficient response to financial crime prevention and detection.

v. Reforming Suspicious Activity Reporting (SAR)

It is a truism to state that that the SARs regime presents challenges to both financial institutions and law enforcement. A significant number of SAR disclosures made to law enforcement are assessed to be of limited intelligence value or are of poor quality. Processing high numbers of low-quality reports which do not improve the investigation of criminal activity diverts already limited FIU resource and is ineffective in driving law enforcement outcomes. This paper certainly does not dispute the necessity of the SAR regime but makes a number of recommendations that seek to enhance its effectiveness.

Improving the feedback loop between FIUs and the regulated sector is key. This would create a virtuous circle that would help reporters to refine their systems and controls and reduce the volume of low-quality SARs being filed. Reducing the volume of

low-quality SARs will help alleviate pressure on FIUs and allow resources to be focussed more effectively. To ensure the feedback loop is enhanced, it is vital that FIUs are adequately resourced and empowered by modern technology.

The effectiveness of the SAR framework could also be enhanced by reforms that would help to optimise the use of resources to improve outcomes. A model that allowed stakeholders to work in collaboration more easily, on suspicions aligned to agreed national priorities would expedite the creation of a comprehensive intelligence picture which would inform and drive the response of all stakeholders against key threats. A SAR 'request' model would allow financial institutions to file a summary of suspicion to the FIU who could then request a fuller investigation if the case was of interest, helping to ensure that a financial institution's investigative efforts were focussed on areas of genuine interest to law enforcement.

vi. Mitigating the inconsistent or incoherent implementation of financial crime compliance standards and guidance, and providing regulatory clarity

The scope of regulatory implementation of financial crime compliance requires careful examination both in the context of jurisdictional approaches and international cooperation. The role of translating the FATF's recommendations into national rules lies with individual countries where cultural, political and legal dissonance can undermine the implementation of a coherent regulatory framework. In some instances, international policy bodies such as the FATF and the Basel Committee have provided overarching guidance and it is important that this is followed up by appropriate statements from national regulators to help remove inconsistencies in the international framework that can be exploited by criminals.

It is also important for the public sector to define and oversee regulatory policy in such a way that empowers financial institutions to implement policies that accord with the government's overall vision of the purpose of the regulatory framework. Clear and consistent guidance from the public sector that is implemented faithfully at the bank examiner level is crucial in this regard and should aim towards moving away from tick-box compliance to focus more on the evaluation of outcomes.

vii. Increasing and improving the use of technology to combat illicit finance

New technologies have bolstered financial institutions' financial crime compliance efforts and hold promise for effective deployment within FIUs. The government of the G20 and the broader international community should encourage the process of innovation in financial regulatory technology that assists in compliance with financial crime regulations and improves risk management overall.

At the same time, examination of barriers to the adoption of new technologies would assist in expanding the risk management toolkit and optimising outcomes. There is a role to play, for example, in expanding access to data for new types of technologies like machine learning.

viii. Conclusion

This paper draws on, and analyses, themes and issues raised during a series of interviews with stakeholders in both the public and private sector. The authors would like to thank those who gave their time and input to what we hope is a useful summary of issues impacting the effectiveness of the financial crime risk management framework and the range of options that, if ideally taken together, would help to improve outcomes and reduce criminal abuse of domestic and cross-border finance.

Overview

The global fight against financial crime is of paramount importance and more needs to be done at the international, regional and national levels to identify and help stem the flow of illicit finance. To explore this issue in greater depth, the IIF and Deloitte canvassed financial institutions, policy makers, regulators and law enforcement authorities in multiple jurisdictions to gauge current perspectives within the financial services industry and the public sector on challenges facing the global financial crime risk management regime.

The formation of this paper combined research with interviews of private sector financial institutions and public sector authorities responsible for AML/CFT and wider financial crime policy and enforcement across Europe, Africa, the Americas, Asia and the Middle East. As such, the paper presents a global outlook on the current state of financial crime risk management, alongside the key recommendations that should be considered to enhance the overall effectiveness of the framework for mitigating the criminal misuse of the international financial system.

While billions have been invested to tackle this problem, greater emphasis needs to be placed on ensuring the legal and regulatory framework and financial crime compliance toolkit are enhanced to achieve better outcomes. A combination of regulatory reform, cultural change and the deployment of new technology could significantly improve the work of governments, law enforcement and the financial industry to counter threats posed by criminal financiers. Financial crime is both a contributor to societal ill and a threat to financial stability and financial inclusion, and its mitigation and prevention must be prioritised. Further action must be taken in an internationally coordinated and coherent manner.

"A combination of regulatory reform, cultural change and the deployment of new technology could significantly improve the work of governments, law enforcement and the financial industry to counter threats posed by criminal financiers."

This paper sets out three areas of focus for both the public and private sector to consider:

1. The systemic stability and societal effects of financial crime
2. Limitations on the effectiveness of the global financial crime risk management framework
3. A way forward on improving the global framework for financial crime risk management

The systemic stability and societal effects of financial crime

More than a decade of regulatory reform in the wake of the global financial crisis has increased systemic stability for international finance. Over the last twelve years, the G20, through the international standard-setting bodies,[1] has achieved the goals of setting higher quality capital standards and mitigating pro-cyclicality; they have reformed compensation practices to support financial stability; established global liquidity standards; and addressed cross-border resolution. Concurrently, enhanced supervision and prudential standards have helped in further safeguarding the overall financial system.

Financial institutions in turn have responded, making significant advances in raising capital, deploying qualified staff for new responsibilities such as recovery and resolution planning, enhancing internal and external reporting, and upgrading corporate governance and risk management standards on a comprehensive basis. In doing so, the financial sector has become more resilient and robust, in terms of holding more and better-quality capital, increased liquidity and less leverage.

While these reforms have helped to mitigate systemic risk and ensure the world is better placed to obviate future crises, risks from sources largely outside the original prudential reform agenda require prompt and coordinated action at a global level. Threats to the operational resilience of financial services firms, fragmentation of markets and the growing pervasiveness of cyber incidents can all lead to systemic stability concerns. At the top of the list for regulators and policymakers working to prevent future shocks to the global financial architecture should, however, also be the real and present threat of criminal incursion into legitimate financial intermediation, including, inter alia, money laundering, terrorist and proliferation financing, fraud, corruption, bribery and embezzlement.

Though this global fight against financial crime is critical, the current financial crime risk management framework is not as effective as it should or could be. The amount of money laundered globally each year, for example, is estimated to be 2% to 5% of global GDP, or between 715 billion EUR and 1.87 trillion EUR.[2] In the European Union alone, less than 1% of illicit financial flows are intercepted, and this does not take into account the fact that illicit proceeds do not always make their way into the financial system.[3] This cross-border criminal finance supports some of the worst problems confronting society today, including terrorism, sexual exploitation, modern slavery,[4] wildlife poaching and drug smuggling.

The scale of the problem and its impact are immense, yet this is not for want of investment in resources to tackle the problem. Corporate and bank respondents to a recent survey indicated they had collectively spent an average of 3.1% of global turnover over 2018 to prevent criminal intrusion into their group wide operations, equating to 1.28 trillion USD.[5]

Financial crime also impacts the most vulnerable members of society and can lead to financial exclusion, in direct contradiction of the goals of the G20 and the wider global community. Corrupt public officials steal from their countries' treasuries and diminish the ability of governments to fund public services such as healthcare and safe municipal infrastructure. Analysis of trade related financial flows in 148 developing nations between 2006-2015 has indicated that on average 27% were potentially related to illicit finance, of which 45% ended up in offshore financial centres.[6] Fraud and bribery contribute to microeconomic impacts such as the loss of business livelihoods and homes. Human trafficking and drug dealing lock the economically disadvantaged into a cycle of dependency with the risk of major health consequences and violence. Studies point to 40.3 million people around the world being the victims of human trafficking.[7] Terrorist and proliferation financiers misusing cross-border money channels put everyone in danger and increase the likelihood of armed conflict.

Human trafficking

The 2018 FATF/Asia Pacific Group paper 'Financial Flows from Human Trafficking' outlines both the enormous human cost of human trafficking and scale of the proceeds of crime generated, which are estimated at 150 billion USD per annum.[8] Case studies illustrate the diverse range of victims, jurisdictions and modus operandi employed by criminal gangs. A common thread throughout is the movement of money and criminal interaction with the global financial system. Payments are made to facilitate crime; for example, to purchase airline tickets that are used to move victims between jurisdictions or to establish adult services websites where the prostitution of victims is advertised. Criminal proceeds from such activities are integrated, moved and reinvested in further criminal activity, including the financing of terrorism. As such the regulated sector has key role to play in supporting law enforcement to prevent and detect this pernicious form of criminality.

The sheer size of the issue poses a risk to global financial stability. For example, the Core Principles for Effective Banking Supervision set by the Basel Committee,[9] the de facto minimum standard for sound prudential regulation and supervision of banks and banking systems, makes it clear that there is an inherent connection between the integrity of finance and the stability of the financial

system. Systemic abuse of legitimate financial channels can lead to reputational risk coupled with a breakdown in customer and investor trust. This can bring about negative macroeconomic consequences when capital flows are disrupted, or liquidity positions of financial institutions are undermined by deposit outflow or through the payment of major fines.

The proceeds of corruption funnelled through the financial system can also weaken countries and governments, especially in emerging economies. A lack of confidence in markets brought on by weak controls which facilitate rampant kleptocracy, for instance, can destabilise inward investment and threaten crucial development projects. Tax bases can be eroded through the funnelling of proceeds offshore or via the intermingling of legitimate economic activity with criminal assets. In addition, if the ability to manage risk in the system is forestalled, certain segments of society can become unbanked leading finance underground via the black market or into the shadow banking system, increasing issues for the facilitation of financial inclusion.[10]

This is not to say that progress has not been made in this area. The FATF,[11] now in its thirtieth year, has led the way in setting international standards and evaluating compliance with those standards to deliver better outcomes for fighting economic crime. The FATF was also the first standard setter to start assessing the effectiveness of their standards in practice and has led the way in in new areas, including, for example, being the first to set standards for virtual assets. Their work is also dynamic and evolving and has, in particular, made vital strides in addressing threats from terrorism.

However, further examination of globally consistent regulatory reform, the use of technology and cultural change could significantly enhance the efforts of the FATF, governments, law enforcement and the financial services industry in tackling the threats posed on a global basis.

Limitations on the effectiveness of the global financial crime risk management framework and a way forward on securing improvement

The financial services industry has invested huge amounts of resource; human, financial and technological, to fight the scourge of financial crime and tackle the issues noted in this paper that ultimately impact the lives of citizens in every country. Likewise, the public sector, and in particular the FATF are working tirelessly to root out criminal behaviour across the globe.

Nevertheless, systemic stability issues for the international community – along with the societal impacts of financial crime – persist and there are several enablers in the anti-financial crime risk management system, each of which has the potential to improve the efficacy of the regime. This paper breaks down those enablers into recommendations for long-term systemic reform and more tactical changes that would allow incremental improvement at pace. Taken together, these have the power to transform how society combats criminality in financial services:

Seven steps to combat criminality in financial services

- Global systemic improvements for financial crime risk management
- Advancing public/private sector partnership
- Improving cross-border and domestic information sharing
- Improving the use and quality of data
- Reforming Suspicious Activity Reporting regimes
- Mitigating the inconsistent or incoherent implementation of financial crime compliance standards and guidance, and providing regulatory clarity
- Increasing and improving the use of technology to combat illicit finance

Work on some of these issues is currently underway at the FATF[12] and elsewhere and others represent a new way forward, but all present a unique opportunity both to improve the quantity and quality of intelligence and insight that is shared between law enforcement and the financial sector domestically and internationally, and to ensure that it is effectively used. Reforms could be used to drive improvements in law enforcement outcomes and the effective application of financial institution systems and controls, shifting the dial away from a threshold based, compliance model to one that is increasingly intelligence led, and outcome focussed and which places entities, networks and behaviours at its heart, on the premise that it is people that commit crime, not bank accounts.

1. Global systemic improvements for financial crime risk management

Background

The current rules for AML/CFT are largely based on a common set of Financial Action Task Force (FATF) standards,[13] however, their implementation can differ across jurisdictions, even when they are applied through a common compulsory national or regional regulatory framework. Issues that arise include; the inconsistent determination of which crimes constitute predicate offenses; inconsistent KYC requirements; barriers to data aggregation; different requirements on which risk factors to consider and how to assess them; varying SAR filing rules; inconsistent approaches to the establishment of beneficial ownership registries and access to information therein. There is also a lack of a common approach to the level of sanctions applied for breaches of the law.[14] Though national competencies must be recognised, financial institutions, regulators, supervisors and law enforcement authorities need to trust that the rules and penalties for non-compliance are congruous. This would eliminate one of the incentives criminals have to channel their operations through jurisdictions they know are less resilient than others.[15]

This inconsistent application of oversight powers by regional and national financial crime supervisory bodies can lead to conflict between rules and a breakdown in cooperation which can contribute to inefficiency and negative outcomes. For example, the European Commission recently recognised that minimum harmonisation of rules at European Union (EU) level coupled with the lack of integration of AML/CFT concerns in prudential supervision, especially in cross-border situations , has led to gaps in the oversight and enforcement regime.[16]

There is also serious global deficiency in the efficacy of financial crime regimes. The FATF assesses the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system and analyses whether a country's legal and institutional framework is producing the expected results.[17] According to the FATF assessment published in September 2019,[18] 75% of the 76 countries reviewed were found to need fundamental improvements when measured against the key goals that an effective AML/CFT system should achieve.[19] Though the level of technical compliance with the FATF Recommendations showed better results overall,[20] the shift from a technical compliance assessment to one assessing effectiveness ,and the subsequent findings of a lack of effectiveness in the implementation of what are the truly fundamental building blocks of a financial crime risk management system , emphasises the global urgency for reform.

Recommendations

Building a better global framework to fight financial crime is a business and societal imperative. To this end, a rebalancing needs to occur, shifting the emphasis away from treating regulatory compliance as an end, but rather as the primary means by which the financial system is safeguarded, and criminals can be thwarted in their attempts to profit from their crimes. The money which flows illegally through the regulated financial services industry gives rise each day to activity which puts citizens worldwide at risk. As noted, there are serious gaps in the system and the public and the private sectors have an essential role to play in addressing these problems. This could be achieved through a better means of tackling risk management for money laundering and terrorist financing and other aspects of financial crime and by reviewing systemic effectiveness:

Review of the effectiveness of implementation of financial crime risk management standards and guidance

Countries and relevant regional/national bodies around the world should examine the effectiveness of implementation of the FATF standards and guidance in their jurisdictions and ensure relevant authorities establish up to date mechanisms to uphold the highest standards and implement those standards in an internationally consistent way.[21] Elements of broader financial crime risk should form part of the Financial Stability Board's (FSB) ongoing analysis of market fragmentation to review gaps in the international consistency of measures designed to mitigate threats to stability that may arise from unchecked cross-border financial criminality, such as issues arising from data localisation.[22]

Findings of inadequacies through the FATF Mutual Evaluation processes must dealt with as a matter of urgency and consideration should be given to further risk-based global assessments in specific areas, such the examination by the FATF of all countries at the same time on such issues as information exchange and access to beneficial ownership information. Concurrently, the FATF should review and build on its methodology for assessing effectiveness and consult closely with the private sector on how the FATF assessments could do a better job of promoting effective action by supervisors, banks and other stakeholders.

Further work should also focus on the need for education, training and technical assistance across all measurements of effectiveness, including for public and private sector stakeholders. The challenge today is not necessarily the absence of standards but rather making improvements to standards where necessary and effectively implementing those standards. This can be improved by education, training and supporting the FATF in holding countries to account.

Increased financial, logistical and structural support for domestic and multilateral public sector anti-financial crime organisations

The G20 has called for increases to the structural support for the FATF. However, given the central role the FATF plays in tackling financial crime, and the importance of coordination with their associate members and observer organisations, the funding, staffing levels and availability of public sector assessors for the organisation should be regularly reviewed to give adequate additional assistance to their important work. This should be coupled with efforts to ensure the correct level of international cooperation is being achieved between the FATF and ancillary regional and domestic AML/CFT bodies and the private sector.[23]

In addition, national governments and regional supervisory authorities should regularly assess the funding levels and structural, staffing and technological competencies of relevant financial crime authorities, national Financial Intelligence Units (FIUs) and cross-border organisations such as Europol and Interpol to add funding and resources where required and to ensure national and international cooperation is effective.[24]

> "Building a better global framework to fight financial crime is a business and societal imperative."

2. Advancing public/private partnership

Background

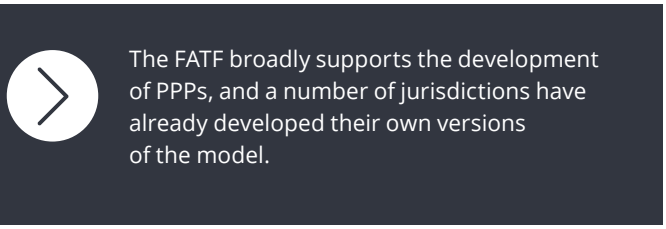
At the centre of an intelligence-led financial crime model which emphasises entities, networks and behaviours sits the public-private partnership (PPP). The PPP is collaboration between financial institutions, law enforcement, policy makers and the regulatory community. Not only are PPPs an important first step in the ability to deliver operational benefits and efficiency gains, but they can also provide a framework to build the relationships and dialogue between stakeholders to help coordinate and catalyse coherent reform of the wider financial crime risk management system.

The FATF has broadly supported the development of PPPs,[25] and a number of jurisdictions have already developed their own versions of the model.[26] They have done so because there is a clear overlap in the interests of all stakeholders in the development of such collaborative exercises which can create a more diverse and fertile basis for pooling information and can more effectively disrupt malign actors attempting to operate through the financial system.

At a conceptual level, a government's 'victim of crime' is usually a bank's 'customer'. The individual is the same person viewed through a different lens, and so both parties, public and private, have an interest and an obligation to work in support of each other in protecting that person and the public more widely.

At a societal level, both financial institutions and law enforcement seek to protect the public from the harm caused by crime. Money is the driving force behind the much of the crime that is committed. By acting in concert with law enforcement to identify and disrupt illicit finance, banks and other financial institutions can make a manifest contribution to the tackling of malicious issues noted in this paper, including terrorism, sexual exploitation, modern slavery, wildlife poaching and drug smuggling, thus protecting the societies and economies in which they conduct business, and in which their staff and shareholders live.

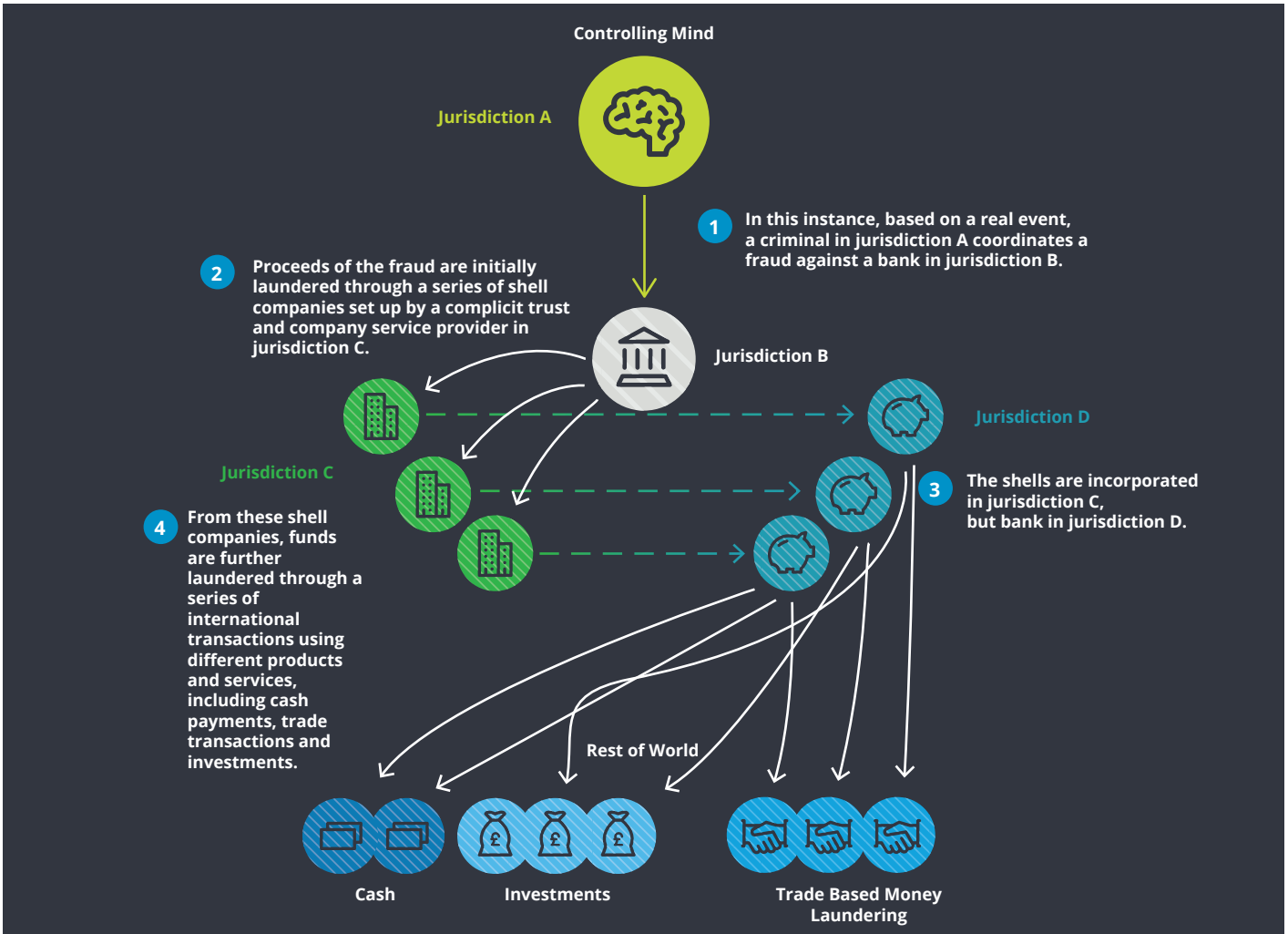
At a practical level, law enforcement needs fast and efficient access to information and intelligence relevant to their case work, while FIs need to understand how they are exposed both to specific and typological risk, so that the risk-based approach can be meaningfully applied in an intelligence-led manner. With appropriate governance and supportive legislation, PPPs can help to address both stakeholders' requirements by providing a safe space in which detailed contextual briefings can be given and discussed. Information shared in such fora can improve the collective understanding of the scale and nature of complex criminal networks, their modus operandi, the individuals involved, the products they abuse, and the jurisdictions with which they are associated.



This information exchange can drive operational outcomes and can provide the opportunity for stakeholders to work with peers to distil collective learning into tightly focussed typologies based on the freshest intelligence. These can then be used to strengthen all parts of the financial crime risk management framework, including training, KYC/Customer Due Diligence (CDD), transaction monitoring and the resultant quality of SARs, improving the overall effectiveness of efforts to detect and prevent further financial crime, while allowing resources to be deployed and technology to be focussed more efficiently on where the risk is highest and greatest impact likely.

The potential value of PPP is illustrated by the early experiences of the United Kingdom's (UK) Joint Money Laundering Intelligence Taskforce (JMLIT) which, since its inception, has supported over 600 law enforcement investigations, contributed to over 150 arrests and the seizure or restraint of over £34 million.[27] Through this collaboration, JMLIT private sector members have also identified thousands of suspect accounts linked to money laundering activity, allowing them to instigate thousands of their own intelligence-led internal investigations. These have in turn led to further focussed referrals to law enforcement, informed assessment of client risk, contributed to internal training materials and helped to identify and prevent further financial crime through implementation of improvements in their respective internal control frameworks. In addition, numerous new typologies have been identified, documented and shared across the wider regulated sector and significant improvements in SAR conversion rates have been observed. These results are encouraging, especially as limitations on how performance data is gathered, for example where it is based on labour intensive manual processes, means outcomes are likely to be significantly understated. Additionally a number of noteworthy results cannot be disclosed in the public domain for security reasons.

An example of a complex money laundering scheme. PPP can help



The Challenge
Complex financial crime is conducted across multiple jurisdictions, institutions and product types. A bank working in isolation is likely only to see a small part of the money laundering scheme, undermining its ability to understand and mitigate its exposure to the wider network. Law enforcement, working through bilateral relationships, cannot know which bank has a footprint and so are hunting blind for intelligence that will progress the case. PPPs can allow stakeholders to develop a fuller understanding of the network quickly so that enforcement and prevention action can be effectively and efficiently targeted. The model would be further enhanced by developments in domestic and international information sharing gateways.

One of the most important benefits of PPPs is also the most difficult to quantify, namely the value derived from the creation of a set of trusted relationships at all levels of seniority around the sense of a shared mission. These relationships create the conditions to drive forward important policy debates, to improve the quality and quantity of feedback between stakeholders, to agree shared priorities and threats which might inform the focus of regulatory expectation and the deployment of financial crime risk management resource.[28] They also help each side to educate the other about their respective capabilities, allowing subsequent enquiries to be tailored accordingly, and enabling operational outcomes to be achieved that would otherwise be missed.

When working well, PPPs can create the necessary conditions to build a foundation of trust which can change the nature of the relationship between government and the financial sector from one that is bilateral and transactional, to one based on principles of cooperation and the effective delivery of a collective whole system response.[29]

Recommendations

Despite good progress made, factors remain that inhibit the further development of PPPs and which undermine their ability to support an intelligence-led approach to fighting financial crime. While the challenges are significant, so is the prize. As such the continued development and integration of PPPs more formally into the financial crime risk management framework as one strand of an increasingly intelligence-led approach is an important priority.

The following issues should be addressed domestically and internationally to ensure PPPs are able to reach their full potential as enablers of effectiveness in the global anti-financial crime regime:

Barriers to information sharing

To be fully effective PPPs must be supported by an information sharing framework that reflects the reality that serious and organised criminals do not operate in one bank or in one jurisdiction. Recommendations on tackling the international nature of financial crime and mitigating fragmentation in the way bank products and services are utilised on a global basis are laid out in section 3 of this paper. However, both public and private sector stakeholders should continue to support efforts to drive and coordinate information sharing reform both domestically and internationally through a governance and legislative framework that balances individual rights with the rights of the public to be protected from terrorism and the effects of serious crime.

Regulatory clarity

Regulators have a critical role to play in the development of PPP. PPPs generally run on a basis of voluntary participation and the support of the regulator is vital in ensuring engagement. While participation in a PPP should not act as a 'golden ticket', in any way absenting a firm from its regulatory obligations or fettering a regulator's power to act, the objectives of a PPP and the objectives of a regulator are broadly consistent when viewed at the strategic level. A properly functioning PPP should enhance the completeness of a financial institution's understanding of risk and the effective application of the risk-based approach, and should reduce overall criminal access to the financial system, both of which are key objectives in any financial crime regulatory framework. It is in all stakeholders' interests to reduce crime, and the PPP model provides an important opportunity to achieve that as part of a whole system approach. As such, regulators and policy makers should consider how best to create the necessary conditions to allow PPPs to flourish and encourage their development.

At a minimum, regulators should articulate that participation in a PPP is considered a sign of a good financial crime compliance culture at a financial institution. This support should be extended to include the increased use of 'regulatory sandboxes' in which the testing and evaluation of innovative intelligence-led models to identify and disrupt financial crime could be trialled in a safe harbour. Arising from this and other experiences, regulators could develop a set of 'golden principles' as to how PPPs could function and could build in metrics and or qualitative assessment criteria to the regulatory framework to encourage and monitor active participation in PPPs to optimise operational outcomes in combatting financial crime and drive efficiencies in operating models.

Over time, and with robust evidence in place demonstrating improved outcomes from an intelligence-led approach, policymakers could review the legal framework underpinning PPP and consider participation in a PPP in the context of a financial institution's wider regulatory requirements with participation incentivised, for example, by reducing burdens in, or automating, technical compliance. This could include dispensation for smaller institutions who may be unlikely to, or were not resourced to, participate in PPPs directly, but still participated in active outreach efforts to law enforcement, attended trainings, symposia, etc. that would increase the effectiveness of their reporting. Grouping regulatory obligation with participation would be a radical step, but one that would have considerable power to incentivise participation in an effective and outcome focussed approach.

Resourcing
PPPs can allow live casework to be proactively shared with financial institutions. This means that any response provided will almost by definition be of value to law enforcement and will be acted upon, something that cannot be said of a SAR regime. At present PPPs tend to operate on a voluntary basis, with staff assigned to handle PPP engagement often being in addition to those required to meet regulatory obligations. This raises costs and may deter engagement in a model that has the potential to increase effectiveness and efficiency within both the public and private sectors. Integrating PPPs within the wider financial crime framework could allow financial institutions to deploy a greater proportion of existing headcount to an area of their response that will more efficiently and effectively identify financial crime while remaining compliant with regulatory obligations.

Evidential use of PPP
At present some PPPs operate on an 'intelligence only' basis because they are not fully integrated into the wider financial crime compliance framework. This means intelligence gathered through a PPP must be separately corroborated through the courts if it is to be used as evidence. This process is inefficient, requiring different teams within banks and law enforcement to process the same information twice. Policymakers and regulators should consider guidance to encourage the use of PPPs evidentially where required for court as this could provide efficiencies for all stakeholders and would facilitate participation. The introduction of a clear legal obligation to share the intelligence when requested by a PPP would assist.

Technology
Volumes of data within the financial sector are growing exponentially as more and more services move online and the world becomes increasingly digitally connected. It is therefore vital that both public and private sector stakeholders continue to invest in technologies that allow the volumes of data generated by modern banking to be analysed and interpreted such that 'big data' becomes a weapon against crime, not an enabler of it. Advanced analytics and visualisation software can identify previously unknown entities and networks to drive the more effective detection and reporting of suspicion, while AI and machine learning could help ensure that lessons learned from casework such as newly identified red flags and unusual patterns, are automatically captured and used to identify risk and inform the development of more effective public and private sector systems and controls.

Cross-sector cooperation
Criminals exploit services provided by a range of commercial sectors and leave a footprint in each. Where PPPs have been established to date, they have generally focussed on developing the relationship between law enforcement and the banking sector, or with other sectors in isolation from the banking sector.

While the development of safe harbour to allow the effective sharing of information between law enforcement and the financial sector is a priority, there are clear benefits in developing the PPP model into one that cuts across sectors so that, for example, lessons learned by banks around the criminal abuse of complex financial products are shared with the insurance sector to inform their understanding of potential risks associated with assets under management, (and vice versa). In addition, a cross-sector approach can also serve to enrich information and provide a more complete picture of financial risks. A bank will, for example, be privy to the value of a transaction, but if it relates to an insurance contract the insurer is likely to be in possession of many more useful details. This type of cross-sectoral cooperation should be prioritised and consideration could also be given as to how it might be extended to non-regulated sectors that may be exposed to money laundering in the fullness of time.

Cross-function cooperation
Today's cyber, fraud and financial crime landscape sees the convergence of criminal activities across these threat areas, with criminals combining their resources, tactics and techniques to commit more crime, more effectively. For example, using cyber-attacks as a means by which to infiltrate an organisation and achieve the level of unauthorised access needed to execute frauds and then launder the proceeds.

It is important that PPPs develop an operating model that draws together the cyber, fraud and money laundering capabilities of its members to tackle illicit activity more comprehensively. By avoiding notional siloes between criminal activities and by engaging the full range of cross functional bank data and capabilities in their activities, PPPs will be better able to fully exploit the power of data aggregation to generate insight and expedite outcomes and opportunities to prevent, detect and respond effectively to the impacts of converged criminal activity.

International collaboration
As referenced in this paper, criminals not only operate without regard to geographic borders, but actively exploit them and the barriers they create. PPPs should continue to build opportunities to coordinate their activities on an international basis against mutual priorities and instances of complex international crime.[30]

3. Improving cross-border and domestic information sharing

Background

The management of financial crime risk can be improved by better sharing of financial crime related information, both domestically and internationally. Such exchange is important to the proper functioning of AML/ CFT and other financial crime prevention policies which fulfil the goal of protecting global finance from criminal incursion. Information sharing is also critical in addressing specific threats that arise from terrorism and proliferation finance. Without adequate insights by financial institutions, law enforcement, and intelligence agencies into the funding of these activities, efforts to stop terrorists and rogue states from inflicting further damage globally will be inhibited.

In the context of the ongoing global dialogue on 'de-risking',[31] 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 restrict, limit or even terminate correspondent relationships. This can further exacerbate financial exclusion for those most in need in emerging markets and limit law enforcement's ability to track illicit money flows.

To overcome these challenges, further efforts are needed to address issues which block operative sharing of financial crime information, including mitigating such issues as inconsistent legal frameworks for data protection, management of SAR-type information, privacy, and bank secrecy, across different jurisdictions.[32]

As noted, improved information sharing is also critical to PPPs. While PPPs offer clear opportunities to improve the collective response to financial crime, a notable feature, (with the exception of the multilateral Europol Financial Intelligence Public Private Partnership),[33] is that all operate on a domestic basis. Even where international banks are members, those banks are bound by local laws and regulations, severely limiting the type of information they can share outside of their institution and across borders.

The limitations imposed by existing information sharing rules are entirely at odds with the realities of criminal operations, which are not bound by – and indeed actively exploit – international borders to evade civil and criminal sanctions. This undermines law enforcement's ability to build a picture quickly and comprehensively, even where established channels such as the Egmont Group[34] or mutual legal assistance exist, and it undermines financial institutions' ability to fully understand their exposure to financial crime risk at a global level. The issues are doubly frustrating in the context of illicit finance as, unlike other crime types, it is often the case that all pieces of the intelligence jigsaw exist and are available in financial institutions, (inter alia, transactions and counterparties), but the dots cannot be connected.

This national approach to a global problem is not only encountered where financial institutions seek to share intelligence with foreign law enforcement, but can even manifest itself within a bank group, where in certain jurisdictional circumstances locally imposed limitations on information sharing prevent information being shared on a group-wide basis as recommended in FATF Recommendation 18.[35]

The FATF is highly cognisant of the issues presented by the limitations around information sharing and does consider information sharing provisions in a number of its recommendations, as discussed below.[36] It has prioritised this issue over the last several years and has made important strides advancing solutions and triggering a global dialogue on improvement. However, further steps to expedite and enhance opportunities around international information sharing for the purposes of tackling financial crime are required. Enhancing the ability to analyse and share data more easily on an international basis would significantly bolster the combined capabilities of the public and private sectors in identifying and disrupting serious, organised crime and terrorism.

Recommendations

Internationally led reform on the facilitation of information sharing is urgently required. However, tactical measures coupled with regional/domestic initiatives will also improve the enabling environment and reduce barriers to the intelligence-led approach in fighting financial crime:

Globally-coordinated reform

At the broadest international level, the FATF is encouraged to continue its important work to improve the effectiveness of its member states' information sharing regimes. Specifically, while the FATF Recommendations offer a comprehensive and consistent framework of measures which countries should implement to combat money laundering and terrorist financing, we believe that the Recommendations would benefit from specific changes to enable more effective information sharing for the reasons emphasized in this paper. Though progress has been made, (as noted), in addressing this issue, as the IIF has previously proposed to the FATF directly, it is suggested that the FATF consider further amendments to the Recommendations which would facilitate these proposals and enable international and domestic group-wide, financial institution to financial institution, financial institution to government and government-to-government information sharing, in all directions.[39]

Implementation of current FATF standards for information exchange

While further broad based reform is needed for the FATF Recommendations to facilitate cross-border data exchange, implementation of information sharing provisions currently in the standards should be expedited by the FATF member states.[40]

For example, it is important to note that there is often an inherent tension between the principles of privacy and confidentiality. The protection of privacy and the fight against financial crime are, however, not mutually exclusive issues. As such, requirements of FATF Recommendation 2 that 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/localisation) is enabled should be implemented across the FATF jurisdictions.[41]

Furtherance of strategic information sharing

While reform across all areas of information sharing should be prioritised, given the need for specific FATF and member state-led action to facilitate such practical exchange, the G20, (and nations beyond that body through their national risk assessment processes) should look for early opportunities to encourage greater facilitation of strategic level information sharing. This would entail cooperation between law enforcement and the private sector on the sharing of specific typologies and geographic indicators of financial crime risk at a national, regional and international level through established PPPs and/or domestic/multilateral cooperation set up to facilitate strategic exchange.

Good typologies, for example, can be hugely beneficial to all stakeholders, allowing financial institutions to focus their investments in detection more effectively on areas of high risk and improving SAR quality. Having produced typologies, however, they must also be effectively distributed. At present there is no robust mechanism by which the collective insight captured in typologies produced is collated and shared with stakeholders on a global basis to inform the collective understanding of financial crime risk and improve the effective and efficient deployment of systems and controls to identify and prevent financial crime. Existing international organisations such as Interpol, the Egmont Group and/or the FATF should consider taking steps to address this issue through the implementation of a global typology coordination function.

Regional and national reform

While further reform of the FATF Recommendations will greatly assist international cooperation and coordination on information sharing, national supervisors and regional bodies should proactively examine where national laws and regulations may impede data exchange for financial crime prevention purposes or where clarifications to those rules through effective guidance could assist with greater data flow domestically and across borders. For example, the US Congress is examining means to expand group-wide information sharing through reform of the US Bank Secrecy Act.[42] The European Banking Authority recently proposed the formation of supervisory colleges to exchange AML/CFT data[43] and the European Commission highlighted in July 2019 the need to review gaps in EU-wide information sharing mechanisms.[44] The Europol Financial Intelligence Public Private Partnership is currently undertaking a review of the rules and regulations for its member countries to potentially help facilitate gateways for information sharing. While a broad, international level approach is key, the G20 and others should also encourage more immediate action at national/regional-level to improve the legal and regulatory environment in this area.

Use of technology

While regulatory reform is an essential component in the facilitation of greater information exchange, the G20 and countries beyond that body should advise national regulators and supervisors to examine how new technology can be used to ease data exchange, and where adoption of such technology can be encouraged within the boundaries of applicable privacy legislation. For example, a financial institution verifying the encrypted data of another financial institution using homomorphic encryption and/or zero-knowledge proof technologies, could enable financial institutions to verify certain types of information with each other, without compromising the security or confidentiality of the underlying data. This is a model being piloted in a number of European jurisdictions. Centralisation of data from multiple institutions into a shared utility, (as noted further in section 4 of this paper), with the data then being centrally analysed for fraud and money laundering monitoring purposes, could also assist.

Sharing of non-personal data

Stakeholders should consider the adoption of a twin track approach to information sharing, with personal data decoupled from the non-personal and processes established to expedite the passage of policy and regulation permitting enhanced sharing of non-personal data. The invariably more complex and nuanced debates relating to the sharing of personal data can be played out at a slower pace.

This approach would represent an extension of concepts already being explored through the capture and publication of beneficial ownership data.

The collation and sharing of non-personal data could be expedited further through the creation of a 'coalition of the willing'. This coalition could comprise a small number of nations with an equal level of commitment to tackling financial crime risk management more effectively, working together and acting in the vanguard, to develop necessary consensus and implement enabling policies and procedures more quickly than would be possible at a global level. This pilot could be used to demonstrate the value of the approach and to create the evidence base to drive the creation and adoption of wider global standards.

Sharing of correspondent data

As noted, most serious crime is international in nature with money moving across borders at speed. Following these money flows presents several challenges to law enforcement, which, if a SAR has been filed, is forced to rely on tools such as international letters

of request or the Egmont Group network to understand what happened to the money at each stage of the laundering process. In the modern world, money can move between multiple jurisdictions in a matter of hours , perhaps even minutes , while the process for law enforcement to catch up can take years, with successful outcomes becoming less and less likely with the passage of time.

An alternative approach would be to allow global correspondent banks greater latitude to share correspondent data with law enforcement bodies, where certain criteria are met, for example; where enquiries relate to commonly agreed priorities such as counter proliferation, CFT and high-end money laundering, and where memoranda of understanding around the use of data have been agreed. The correspondent banks could use their insight into global money movements to guide law enforcement rapidly through a network of international payments and expedite opportunities to identify the ultimate destination of criminal money flows. This would increase significantly the probability that those funds could then be restrained or seized by law enforcement through an intelligence-led, targeted judicial order.

Making better and more coordinated use of correspondent banking data has the potential to improve outcomes against the most serious money laundering networks and criminal gangs. It could also be used to better inform the collective understanding of money laundering typologies, to inform risk assessment of products, services and jurisdictions, all of which could be used to inform a more effective implementation of the risk-based approach in banks and would inform collective efforts to prevent crime and take it out of the system.

The Multinational SAR

Existing limitations on international information sharing routinely prohibit an international financial institution from sharing its global view of a criminal network with a national law enforcement body. The effect of this is that a single institution's comprehensive picture of the issue must be broken up, with fragments of that picture filed separately in different jurisdictions.

There are mechanisms through the Egmont Group for law enforcement to reassemble that single picture, but they are time consuming and predicated on the assumption that one jurisdiction already knows that relevant material has been filed elsewhere. There are also risks around loss of data fidelity, because, as the picture is reassembled, each jurisdiction assesses what proportion of the information can be shared without redaction, with key details or context often stripped out.

The net effect of these limitations on information sharing is that the law enforcement agency investigating the case is likely to receive only a partial picture of criminal money flows after the filing financial institution had already compiled a comprehensive picture. The financial institution incurs costs building the intelligence picture, and then further costs in breaking it apart and filing it separately in multiple locations. Law enforcement incurs financial and opportunity cost in attempting to reassemble an imperfect version of a picture that previously existed in complete form. This process benefits only the criminals.

Nations with a commitment to tackling complex financial crime should consider how better use may be made of a global financial institution's initial, potentially comprehensive, insight into an instance of global financial crime. If, for example, a global bank's SAR contains data from five jurisdictions, the whole SAR could be filed in its entirety in all five jurisdictions, so that each jurisdiction knows the others have a potential interest and steps can be taken to act in collaboration to tackle the issue.

This approach is challenging in that it assumes both a degree of global coordination to amend SAR frameworks, (further discussion on SAR reform is covered in section 5 of this paper), and the political will to review legislation where it prohibits personal data being shared beyond national borders, something that would be at odds with current legislative frameworks in a number of jurisdictions. However, progress could be made by employing an approach similar to that described above in relation to the sharing of non-personal data, with countries working through bilateral arrangements or in small groups with trusted partners to allow their banks to file information relating to each other's jurisdictions in jointly filed SARs.

The beneficial impact of developing a multinational SAR would be significant. It would ensure investigators in affected jurisdictions receive a comprehensive overview of an international criminal network quickly, facilitating collaboration to trace assets and disrupt criminal activity, while reducing costs to banks through increased efficiency. Multinational SARs would also help to ensure that new and complex money laundering typologies were more quickly and efficiently identified and shared, allowing preventative action to be more effectively implemented on a coordinated basis. The concept of a multinational SAR would be particularly powerful if those nations hosting major financial centres were to be early adopters as this would ensure that a significant proportion of global suspicion could be captured and shared in single reports.

The Common Reporting Standard

The introduction of the Common Reporting Standard (CRS) allows confidential and personal data relating to taxpayers to be shared between jurisdictions.[45] Many of the arguments made regarding the introduction of the CRS would apply equally to the tackling of money laundering, tax evasion being a global problem that requires a global solution. Policy makers in the financial crime space should revisit the arguments made in support of the creation and implementation of the CRS to leverage the model and expedite the implementation of similar information sharing powers in relation to other financial crimes and terrorist financing.

Where better information sharing would have helped the fight against financial crime

A number of significant money laundering cases have been publicised in recent years, including, for instance, the Russian Laundromat, the Fortuna fraud, Mirror Trading and the Panama Papers. These cases, and others like them, illustrate both the scale and complexity of money laundering schemes and the ease with which the proceeds of crime can be transferred between jurisdictions.

By way of example, the Moldovan laundrette scheme is assessed to have moved at least 20 billion USD[37] of illicit funds from Russia into the global financial system before it was revealed in 2014. The scheme employed a complex network of hundreds of shell companies, nominee directors and international bank accounts across a range of jurisdictions. Fictitious loan arrangements were created between shells incorporated in the UK but banked in the Baltic states. These loans were in turn guaranteed by further shell companies in other jurisdictions.

The loan agreements were then defaulted on with the subsequent dispute resolution played out in the Moldovan court system that could claim jurisdiction because Moldovan nationals were nominally in control of the shells involved in the dispute.

The courts would find in favour of one side or the other and instruct that the loan be repaid by the overseas shell acting as the loan guarantor. The value of the loan, (sometimes hundreds of millions of dollars), would then be transferred to the Baltic bank account of the shell company assessed to have 'won' the dispute.

The controllers of the network were able to use the adjudication of the Moldovan court to explain the source of wealth, and bypass CDD controls that may have been alerted by the incoming payment at the receiving bank in the Baltics.

Money was then transferred out into the global financial system through onward cash payments, trade-based money laundering schemes and investment in other financial products.

While several jurisdictions have instigated investigations into these and other schemes, and in some cases, have affected law enforcement or regulatory action, there remains a stark imbalance between the scale of the alleged criminality and the scale and impact of the response. Of the billions that are alleged to have been moved, very little has been traced, restrained or seized, and very few arrests made, or prosecutions secured.

While this may be dispiriting, it is not surprising. Money transferred through schemes such as these can move opaquely and rapidly through multiple jurisdictions in a single day, while tracing those flows can take years. This creates an inequality of arms between law enforcement and criminals that can only be improved through substantial reform of international information sharing rules and the more effective exploitation and networking of siloed public and private sector data internationally. International policy making bodies such as the G20 must continue to drive such reforms.[38]

4. Improving the use and quality of data

Background

The use of data can be transformative. How it is stored and accessed can be as important as its flow through effective information sharing mechanisms. There is a degree of consensus around the importance and benefits of collating, standardising and making available contextual datasets through utilities that support a consistent 'single version of the truth' and which can be used by financial institutions to fulfil key KYC and CDD requirements, along with other proactive investigative financial crime requirements and obligations.

Having a single, reliable, independently verified source for such information would have considerable beneficial impact on the volume of resource currently expended in this area and would ensure consistency and quality in terms of what was gathered and made available to financial institutions in order to complete their KYC obligations. At present, the fragmented KYC data landscape is characterised as one of information asymmetry, whereby different financial institutions, possibly even branches and subsidiaries within the same group, each hold information on the same customer which may overlap, but which may also be inconsistent and incomplete, a weakness which criminals can navigate to exploit the financial system.[46]

Contextual data sets built on a single verified 'golden source' are a potential solution to this issue and the arguments to support their creation are compelling. The deployment of such utilities could substantively streamline onerous capital, and labour-intensive efforts that are currently expended in creating and recreating fragmented and partial views of the customer through the provision of reliable and accurate customer information in an efficient manner, employing a principle of 'do it once, and do it well'. They could also act as a driver for the sharing of best practice and the collective raising of the financial crime compliance bar.

There are, however, significant challenges to the design and implementation of shared or 'mutualised' contextual data sets and their supporting utilities. These include the high financial start-up and integration costs and the fact that current liability models do not reflect the shift in responsibility and accountability for risk that underpin shared utilities, as well as concerns surrounding the management of data privacy and operational risk.

Recommendations

Areas of priority regarding the centralisation of data include the development of registries of beneficial ownership, common utility models for KYC/CDD, the use of digital identity and greater data fusion and pooling within organisations.

Corporate information centralisation through beneficial ownership registries

FATF Recommendation 10 (b) states that in the case of customers who are legal persons or arrangements, financial institutions should identify and take reasonable steps to verify beneficial owners, and "should include financial institutions understanding the ownership and control structure of the customers."[47] This is capital and labour intensive and duplicative in that it is often the same entities whose structures must be independently identified and re-created multiple times by different on-boarding, CDD and financial crime operations departments. Moreover, the application of different standards and procedures when conducting CDD on customers and their corporate structures can result in inconsistent information being gathered by financial institutions. This asymmetry is not lost on those who would seek to exploit such gaps in the financial system to launder the proceeds of crime. Criminals are aware that financial crime compliance operates in a siloed manner dictated by the inherently territorialised nature of legal regimes and regulations, both those directly related to financial crime and those that govern the retention and sharing of information such as data privacy and bank secrecy laws.

In the wake of the Panama Papers and Paradise Papers scandals,[48] beneficial ownership registers have gained prominence as desirable contextual dataset to facilitate greater transparency around the ownership and control structures of corporates. The concept of beneficial ownership registers is embedded in the FATF Recommendations[49] however progress in the implementation is uneven across the globe, and where it is made available, a common theme is that the data is held and maintained by a public body, that lacks the financial and human resources to effectively police the quality of the data.[50] This issue needs to be addressed through policy change and investment.

While the FATF makes clear that countries should be responsible for ensuring that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons, it can be with a view to making this available for the benefit of law enforcement and competent authorities. As such, this should be extended to the regulated sector more widely , where this is not done already, to enable it to become a significant 'force-multiplier' in what is considered one of the most challenging areas of the KYC process.

- Harmonise and allow reliance on accessible, verifiable and up-to-date beneficial ownership registries on a global basis: Beneficial ownership regimes require greater harmonisation and consistent implementation on a global basis. Where a robust platform for accessing information on underlying control of linked entities does not exist or is impaired by laws and regulations which cause silos in information exchange, systemic weakness can develop. Accessible beneficial ownership registries should be implemented around the world consistent with FATF-developed guidance.

  An important point that has not been fully addressed on a global basis however, is the issue of upon whom the burden of responsibility lies to identify beneficial ownership. Much of the onus historically has been on financial institutions to identify and verify this. There should be an increased emphasis on requiring the legal entities themselves to be more forthcoming in a verifiable, public way. Independent, public and reliable registries should be encouraged, actively policed and backed by governments as a reliable source of due diligence information. Governments should stand by the contextual reference data they provide, ensuring it is a 'golden source' upon which the regulated sector can rely both practically and legally.

  In addition, the use of the Legal Entity Identifier (LEI)[51] should be considered to enhance methods and tools for transparency. The LEI provides for the unambiguous identification of legal entities and could be effectively leveraged by law enforcement and regulators in identifying the actual entity that owns a structure or in monitoring. Incorporating further use of the LEI into registries as a required field and encouraging its use would aid in securing further reliable information on overall control and enhancing customer due diligence generally.

Mutualisation and centralisation of data through common utilities

In order to tackle the problem of information asymmetry generated through the current compliance model, whereby each financial institution, (and even different business areas within a single financial institution), works in isolation to collect and collate KYC information, it is necessary to establish consensus on what constitutes the single version of the truth about each customer. One approach would be to mutualise customer information, such that the utility retains a single KYC record that is then available to the different financial institutions using the services of the utility. A number of jurisdictions have developed early incarnations of such utilities with differing levels of success. These include Singapore, the Nordics, the Netherlands and 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 for the conduct of customer due diligence on African entities in order to alter risk perceptions, address de-risking on the continent, and promote trade in Africa.[52] The financial industry has already taken the initiative to establish a globally recognised KYC standard, and has built the KYC Registry.[53]

De-centralised models are also conceptually possible, and implementation of these models could be enhanced through ongoing developments of distributed ledger technology. Expediting the development and implementation of utilities however requires a number of enabling factors, including:

- Improving private-public collaboration on utilities: Close cooperation between the private and public sectors, (including regulators), is vital to ensuring that the resulting utilities effectively address not only the bespoke requirements of each financial institution, but also the legal and regulatory framework of the jurisdiction in which the utility model is established.

- Recalibrating the liability model: Financial institutions continue to be accountable for the accuracy of the information collected on their customers, even if that information is obtained from official sources such as company and beneficial ownership registries. The EU Fourth Money Laundering Directive,[54] for example, makes clear that this information should not form the sole source upon which financial institutions should rely in order to satisfy their customer due diligence obligations, and that those requirements shall be fulfilled by using a risk-based approach. The onus, and therefore the risk regarding the accuracy and quality of this information, rests with the financial institutions. The pressure on financial institutions to invest resourcing in getting this critical element of the KYC process right, is significant and risks inculcating a 'tick box' compliance culture that diverts resource from potentially more effective intelligence-led approaches to the tackling of financial crime.

The development of utilities in close collaboration with regulatory authorities should therefore be accompanied by a distribution of accountability for risk that seeks to adjust the current model where the onus lies solely on financial institutions. The development and use of 'golden source' data in collaboration with regulators and other public sector bodies should be supported by an explicit understanding, enshrined in law, that financial institutions will not be held liable for the veracity and provenance of that data, (a distinction from the continuing obligation to undertake due diligence in a manner commensurate with the risk profile of the customer). The relevant public sector bodies must share some of the responsibility for the quality of the data, along with greater emphasis on legal entities to provide better quality KYC data on themselves, (e.g., greater transparency and accuracy of data around beneficial ownership).

Embedding digital ID into financial crime risk management frameworks

Digital identity has the potential to be an important category of mutualised data at the heart of financial crime prevention. At the level of the individual, the digital evaluation of identity documents could reduce document fraud and enhance confidence in KYC processes, while simultaneously expediting the customer on-boarding process. Digital identity could also be extended to include the verification of corporate ownership structures which could then be reliably reused, for example, when applying for new products and services in that or another financial institution.

Digital identity also has the potential to enhance privacy by enabling individuals and organisations to share only the information required to complete a transaction, removing oversharing of information simply because it is embedded within paper-based identity documents. The use of zero-knowledge proofs can extend this protection by removing the need to share any of the underlying information.

While digital identity has the potential to improve the efficiency and effectiveness of financial crime risk management frameworks, the extent to which it will be adopted will depend on several factors. These include the clarification of regulatory uncertainty around the legal use and acceptance of digitally verified credentials and the development of the necessary governance protocols to ensure widespread trust in any globally interoperable digital identity model.

Currently, the lack of clarity around what are acceptable forms of digital identity means organisations will be operating in a grey area as to whether digitally verified credentials are an acceptable form of identity. This creates a real or perceived regulatory risk which drives organisations towards the continued use of traditional forms of identification.

A second limiting factor is the broad range of emerging digital identity ecosystems with centralised models perhaps easier to govern, but decentralised models offering international scalability and increased security against, for example, cyber-attacks.

The potential value of digital ID, as both a means by which to improve both the efficiency and effectiveness of the KYC process which is at the heart of all financial crime risk management frameworks, is significant. As such both international standard-setters and national authorities are encouraged to examine the issues above and provide guidance on which models of digital identity are or are not acceptable so that in time the collective benefit of digital ID in fighting financial crime can be harnessed.[55] We note the good work of the FATF already in this area in developing guidance on the use of digital identity for the purposes of conducting customer due diligence and such means of international coordination should be encouraged.

Data fusion/pooling

Another important enabler of an effective and efficient response to financial crime compliance is data fusion. Many organisations work in silos, collecting data and building systems to tackle crimes such as money laundering, fraud, sanctions evasion, cyber-crime and market abuse separately.

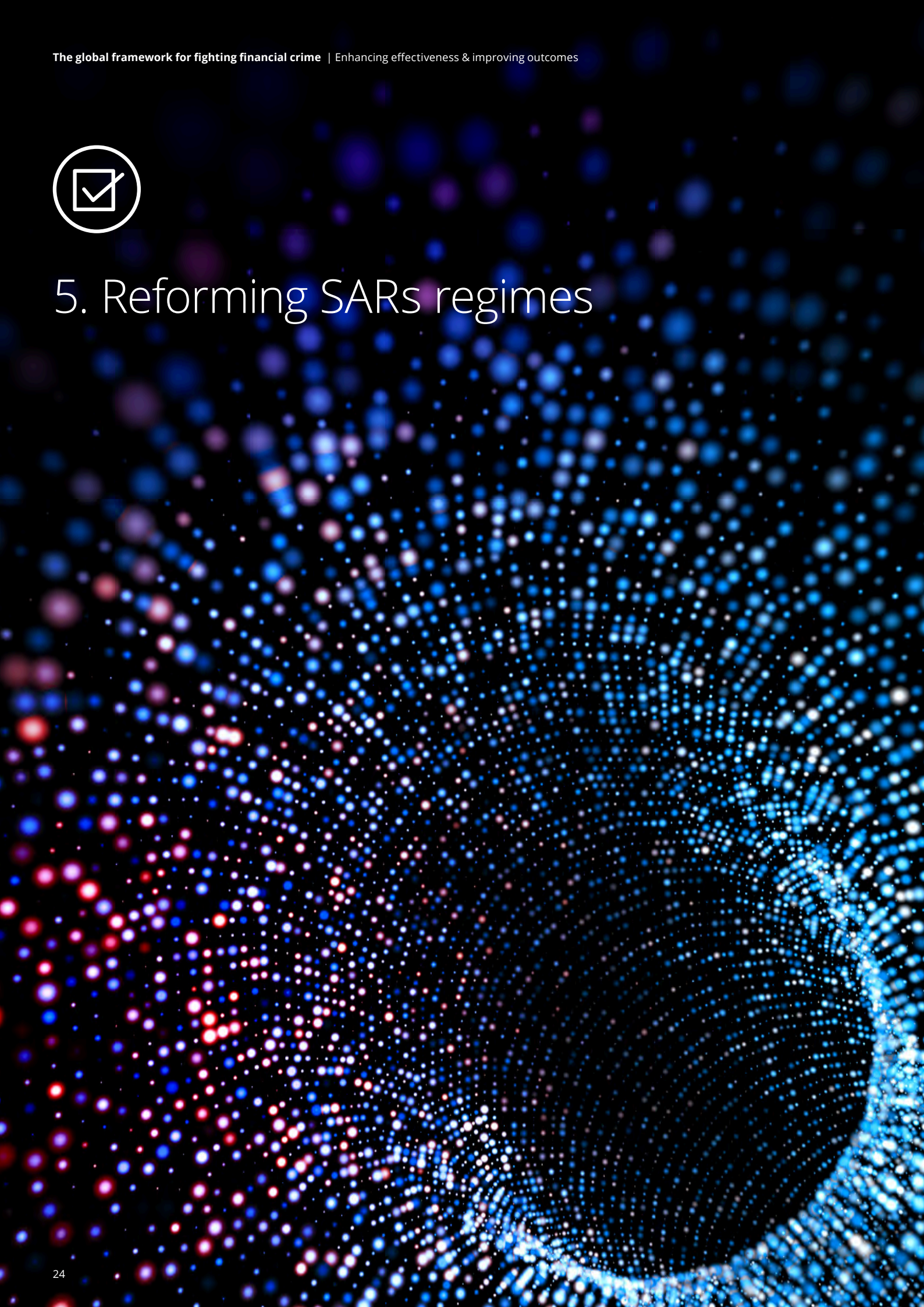
Criminals do not operate exclusively within these thematic silos, instead operating cross-domain and cross-border to make money and evade detection. For example, a cyber-attack may be used to obtain confidential data, which is then used to commit fraud, the proceeds of which are laundered.

Indeed, criminals are likely to leave traces across a Financial Institution's compliance functions. Equally, a criminal may have entirely legitimate interactions with the bank, running a 'clean' life in parallel to their criminal one. If data is not reconciled across the bank, any assessment of risk will not be fully informed and opportunities to detect and prevent crime efficiently and effectively may be lost.

Data reconciliation or fusion is a key enabler to the effective delivery of the wider reforms discussed in this paper, including PPPs, financial institution-to-financial institution information sharing and better use of SAR data. All these reforms drive towards a future where there is an increase in the volume of intelligence and insight flowing between stakeholders in the financial crime compliance community so that investment in resources and effort can be made expeditiously. If financial institutions are not able to interrogate that intelligence across their entire data holdings, opportunities will be lost.

- Support greater pooling of data: Data fusion offers a range of benefits in addition to the more efficient and effective detection of crime. It can deliver inherent cost savings, allowing multiple versions of similar systems such as case management and analytics tools to be rationalised. Fusion can allow a financial institution to build a more comprehensive understanding of risk, so that exposure to regulatory sanction, as well as private litigation, is reduced. Finally, a holistic customer view allows organisations to make insightful and data-driven decisions, tailoring products and services to customers as required.

5. Reforming SARs regimes



Background

It has become a truism to state that that the SARs regime presents challenges to both financial institutions and law enforcement. The volume of monitoring alerts generated, investigated and, where appropriate, disclosed represents a significant operational undertaking, creating financial and resourcing pressures on the filing institution. A 2018 study looking into the resources devoted to the Bank Secrecy Act (BSA)/AML compliance in the United States found that the 18 respondents surveyed devoted an average of 22% of their BSA/AML dedicated compliance resources to the SAR function, accounting for the single largest resource component of their BSA/AML compliance framework.[56]

A product of this investment is significant numbers of disclosures made to law enforcement. For example, in the period 2016-17 over 400,000 SARs were submitted to the National Crime Agency (NCA) in the UK alone.[57] However, according to the FATF UK Mutual Evaluation findings from 2018, there were only 80 staff on average in the UK FIU to deal with all the SARs submitted at the time of the FATF review visitation in March 2018. The disparity between FIU resource and the quantity of SARs submitted is a frequently noted issue in several jurisdictions. Even though some countries operate a 'distributed model' with SARs made available to the wider financial investigator community, it is still the case that the public sector does not have enough resources to investigate all disclosures; and to a degree, nor should it, as quantity of SAR filings does not always equate to quality.

Huge volumes of SARs of low-quality drive poor outcomes and waste valuable resources. Poor outcomes are mirrored in poor conversion rates. A Europol report published in 2017 looking at the effectiveness of the SAR regime across the EU found that between 2006 and 2014, the rate of disclosed SARs that were subsequently converted into further action was between 10%-14%.[58] In addition, the proceeds of crime that were provisionally seized or frozen were estimated to be no more than 2.2% for the period 2010-2014. Given that disclosures constitute one of the principal means for generating intelligence for law enforcement to investigate and prosecute crime more generally, getting this right is critical for any effective intelligence-led financial crime compliance model.

Recommendations

This paper describes a number of reforms to improve flows of intelligence and insight between stakeholders in the financial crime compliance community, including increased use of PPP and reforms to information sharing rules. The regulated sector is the frontline in the fight against financial crime and increasing the volume of intelligence and insight shared will allow the private sector to implement the deployment of their assets and effort where it is most needed as part of a genuinely intelligence-led risk-based approach, that will prevent more crime and generate more meaningful SARs focussed on priority areas that have a higher likelihood of being reviewed and actioned by law enforcement. These improvements would be further assisted by greater transparency around regulatory expectations regarding reporting.[59] The recommendations presented below are not designed to dispute the necessity of the SAR regime, but rather seek to improve its effectiveness through harnessing intelligence to ensure optimisation of the process and the quality of disclosures.[60]

Priority SAR model

One option to enhance the effectiveness of the collective response to financial crime would be to better enable public and private sector stakeholders to work collectively against criminal threats that had been commonly agreed as national priorities – for example through a process of national public/private threat assessment.

Where reporting institutions identified suspicion that related to one of the national priorities, they would notify the authorities who would have the power to invoke an expedited information sharing process underpinned by clear enabling legislation. This legislation would permit public and private sector stakeholders to work proactively and directly with each other, including as part of a co-located 'taskforce' to identify, pool and analyse relevant data, with a safe harbour from wider rules and regulations governing, for instance, client confidentiality and data privacy. The authority to trigger enabling legislation could rest with the FIU or the regulator and would be governed by an assessment of proportionality, necessity and justification.

The 'priority SAR' approach would seek to balance the tension between privacy and investigation through alignment of capabilities and national priorities. It would also enhance existing SAR regimes, based primarily around a single institution, reporting with the power of the collective helping to ensure that the most serious threats to society were dealt with effectively in a manner that was consistent with a risk-based approach.

A SAR 'request' model

At present SAR reporters are provided with limited feedback about the relative importance of the suspicion they have identified. As such reporters are often not sure about whether their report is of high or low interest to law enforcement or the FIU.

In the absence of this context, reporters will expend an equal amount of effort on the investigation and reporting of all suspicions rather than focussing resource on those cases that are of greatest interest or significance to law enforcement, in effect diluting the total resource applied to priority cases.

A more efficient solution would be to amend reporting requirements so that initial 'notifications of suspicion' to the FIU are simplified, perhaps limited to core customer data and a synopsis of the suspicion, with the bulk of a reporter's investigative capability held in reserve for priority cases.

The FIU would consider each 'notification of suspicion' upon receipt and if the entities or topic it related to were of particular interest, could request that the reporter instigated and reported a full investigation which would be completed to agreed timescales and to an agreed and comprehensive standard. This approach would allow both private and public sector stakeholders to ensure that maximum effort was focussed on areas of the greatest importance to law enforcement, improving the efficiency and effectiveness of the system overall. Conceptually, the idea of a 'Request SAR' could be extended further and even partially automated over time, with banks provisioning law enforcement with direct access to underlying data relating to the suspicion that had been filed.

Improve the 'Feedback Loop'

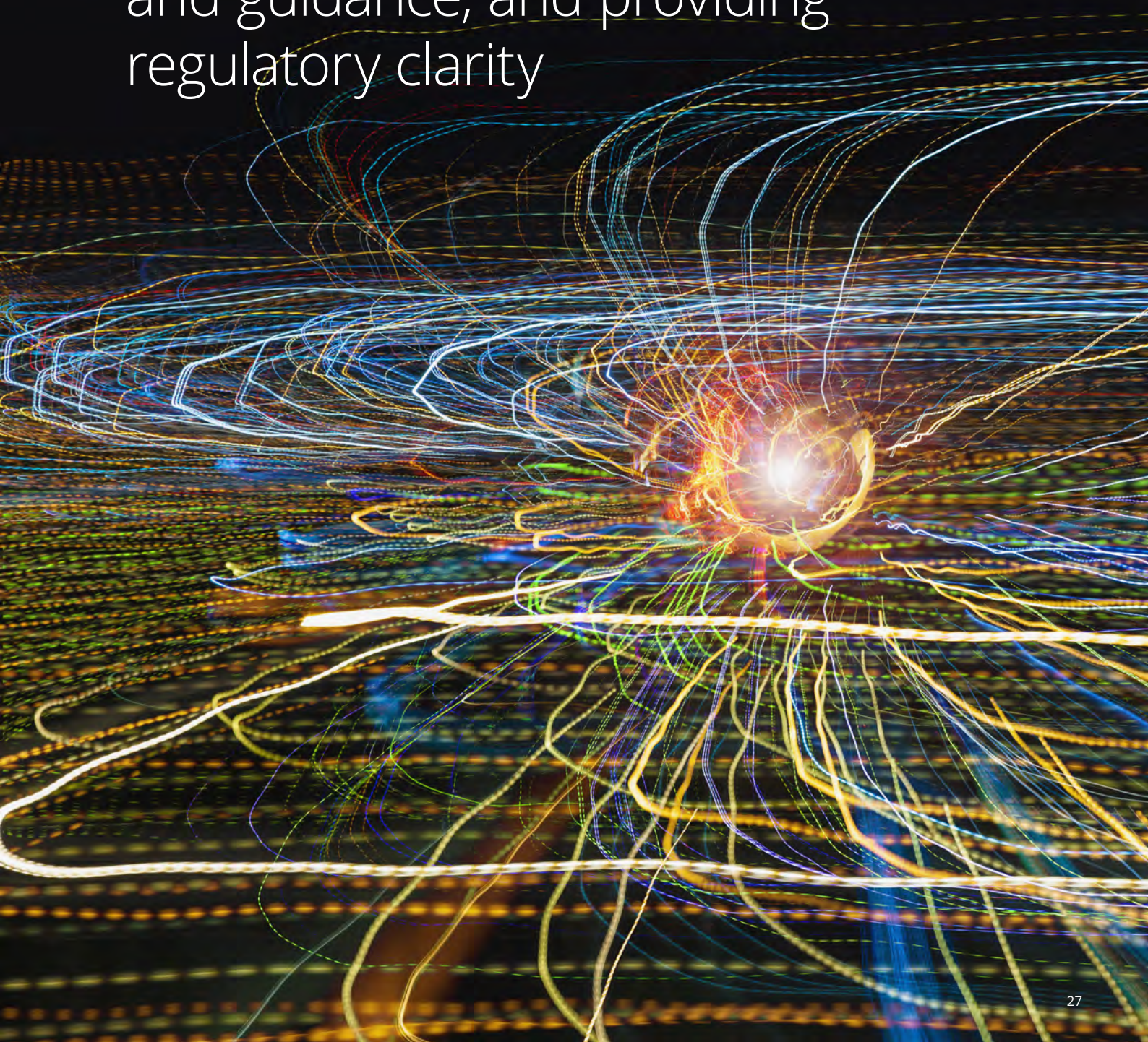
A crucial factor in improving the quality of SAR disclosures would be to increase feedback from law enforcement to the reporting institutions. The absence of feedback provided by law enforcement once a disclosure is made is a common issue and is one that has arisen in most jurisdictions. Where little or nothing is communicated back from law enforcement/FIUs, reporting institutions are less able to refine their own approaches to the identification of suspicious activity or improve the quality of reports filed. As a result, institutions are not made aware of where they are failing and, consequently, how they can improve.

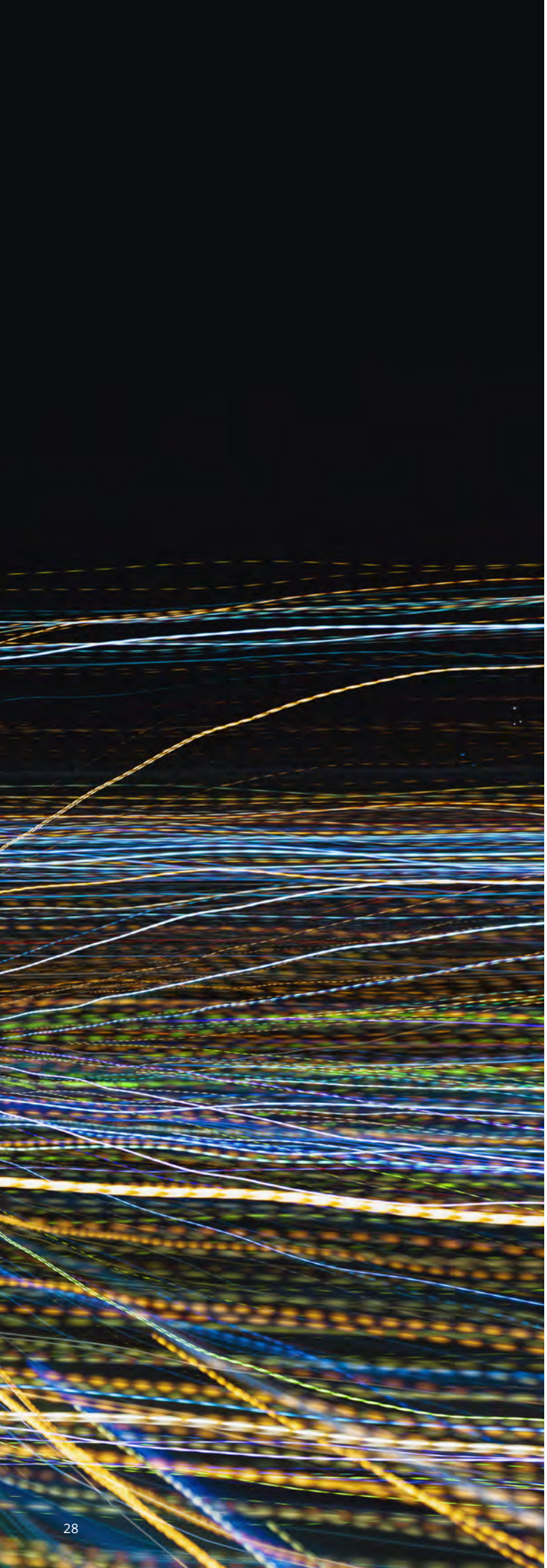
- Debrief of complex cases: The privileged position held by the FIU at the centre of the SAR system potentially provides access to a more comprehensive overview of a complex multi institutional money laundering scheme than would be available to reporting institutions working in isolation. In these circumstances, what may seem obvious to the FIU, may not be to reporting institutions. It is vital that FIUs do more to share learning derived from analysis of complex cases in addition to wider threat and trend analysis so that the reporting sector can more effectively focus its resources informed by a better understanding of the risks.
- Collective upskilling: Increased dialogue between the regulated sector, law enforcement and the FIU would enhance the skills, capabilities and awareness of all stakeholders involved in the SAR lifecycle. For example, briefings from private-to-public could help law enforcement staff to better understand the characteristics of complex financial products and services, so that when disclosures are made involving the use of such products for money laundering, law enforcement is better equipped to understand how they have been exploited and to take appropriate action. Public-to-private briefings could provide, inter alia, insight on priorities, the key elements of a 'good SAR' and emerging threats.
- Automation: Automation within the SAR process could function as an accelerator; helping to drive efficiencies in the processing of alerts and unusual activity reports, and in identification of suspicion. Depending on its nature and extent, automation could be applicable to both threshold based reporting , characteristic of transaction monitoring, and to unusual activity reports that are primarily the domain of human input and judgement.

  It is important that the regulatory community supports and encourages the exploration of new, and potentially more effective, ways of working to prevent and detect financial crime, including, for example, the application of concepts such as Artificial Intelligence and automation as discussed in greater detail in section 7 of this paper.
- FIU resourcing: It is vital that FIUs are adequately resourced if the investment currently made by the regulated sector in the identification and reporting of suspicion is to be fully realised through effective analysis which would drive both improved operational outcomes and a more effective feedback and prevention loop to reporters. However, gaps exist on a global basis.[61]

  The potential value of secondments between the private and public sectors has been widely acknowledged as mean to improve outcomes on both sides. A secondment model for FIUs with appropriate governance in place would offer value to both public and private sector stakeholders. The FIU could use such a model to source additional capacity without incurring significant additional resource costs. The private sector would benefit from a cadre of staff who would bring back a deep and practical knowledge of the workings of financial crime and an enhanced understanding of government ways of working and priorities, all of which could be used to direct their firm's wider investment in financial crime risk management controls.

6. Mitigating the inconsistent or incoherent implementation of financial crime compliance standards and guidance, and providing regulatory clarity





Background

Regulatory implementation of financial crime compliance regimes requires careful examination. The inconsistent application of the global standards can create loopholes that can be exploited by criminals and can create conflicts between regimes that undermine effective international cooperation. It is equally important that financial crime risk management frameworks are implemented and regulated in such a way that they promote and prioritise the effective delivery of outcomes and do not view technical compliance as an end in itself.

Recommendations

A combination of coherence in international and domestic standards and clarification of regulatory expectations would improve the consistency of financial crime risk management regimes, and would also make for more effective financial crime compliance frameworks within financial institutions:

Reduce ambiguity and divergence in financial crime regulation and policy

Ambiguities that exist in international financial crime regulations leave significant room for interpretation and can lead to fragmentation among jurisdictions with conflicting sets of requirements. For example, some jurisdictions do not specify which crimes can serve as predicate offences for money laundering prosecutions. Agreement on and uniformity of customer due diligence practices in financial crime policy is also lacking, and there are still uncertainties in some areas as to the validity and applicability of 'know-your-customer's customer' (KYCC) obligations on financial institutions and the possible liabilities arising from noncompliance with such requirements.[62] This can exacerbate issues with 'de-risking' in the international financial system, a situation which can have significant adverse consequences for the goals of the G20 in increasing financial inclusion.

The FATF and the Basel Committee have taken steps to provide additional guidance on some of these issues, including KYCC, in the context of the correspondent banking market.[63] However, as noted by the FSB,[64] the FATF and Basel Committee guidance should be followed up by statements from national regulators clarifying expectations domestically so that they are appropriately reflected in supervisory practices and banks' risk management programmes.

FATF guidance on established recommendations or principles can only go so far in providing the regulatory certainty needed by both the private sector and national authorities. Still, it must be applied in good faith across member state jurisdictions for it to be fully useful. Guidance is generally non-binding and can sometimes even be invalid due to contradictory rules in effect in certain jurisdictions. It is incumbent on national authorities to clarify regulatory expectations as to its ultimate effect. A means of ensuring FATF Guidance is adopted in a fulsome and transparent fashion across jurisdictions is ultimately needed, otherwise there is a real risk the status quo will be maintained.

Clarify regulatory expectations

There is a need for the public sector to define and oversee policy in a way that empowers financial institutions to implement the government's vision. Clear and consistent guidance from the public sector that is implemented faithfully at the bank examiner level is crucial in this regard. The transposition of the regulatory regime governing financial crime into an actionable compliance programme can, at times, be hampered by the dissonance between a regulatory expectation centred on detection, prevention and disruption of financial crime, and an assessment framework that focuses on the extent to which a financial institution's financial crime compliance programme is technically compliant.

For example, in the United States, the Federal Financial Institutions Examination Council's (FFIEC) BSA/AML Examination Manual focuses on banks' financial crime compliance programs rather than providing opportune and actionable intelligence to law enforcement. The emphasis on being technically, or formally, compliant appears to be driven by proscriptive criteria wherein each element in that suite of measures is treated equally and without consideration for the fact that some measures will play a more pivotal role in mitigating financial crime risk than others. This can perpetuate a financial crime compliance culture that privileges a 'tick-box' compliance exercise rather than one that is driven by, and measured against, the strategic objectives of detection, prevention and disruption.

The discrepancy between the imperatives of evaluating the minutiae of a bank's financial crime compliance programme rather than its operational effectiveness can lead to the focus of a significant proportion of resources on ensuring that programs satisfy the expectations of the examiner.

To this end, the public sector needs to lead the way on two levels. First, it needs to articulate clearly, consistently and transparently what the regulatory expectations are, and how these are transposed into the criteria to be used in evaluating whether a financial institution's financial crime compliance programme satisfies not only the financial crime risk management regime, but also its effectiveness in assisting the authorities in meeting their strategic financial crime objectives.

Secondly, regulatory expectation and its evaluation in a bank's financial crime compliance framework needs to factor in the evolution of banking practices that have outpaced regulation as well as technological developments, particularly in terms of the tools that financial crime compliance functions are able to develop and deploy in mitigating their exposure to financial crime and detecting when and where it may be occurring. How and what is evaluated when assessing a bank's financial compliance program needs to consider this changing landscape and to do so in a manner that foments and encourages, rather than stifles or impedes, the flexible and innovative approaches that banks may explore in meeting government vision and regulatory expectation. There are nascent signs that these considerations are beginning to be taken on board by key public sectors actors.[65]

"The inconsistent application of the global standards can create loopholes that can be exploited by criminals."

7. Increasing and improving the use of technology to combat illicit finance

Background

New technologies have dramatically bolstered financial institutions' financial crime compliance efforts and hold promise for effective deployment within FIUs. Machine learning and AI technologies have the potential for self-learning and analysing large amounts of complex data and are improving monitoring and analysis of suspicious activity on financial institutions' client accounts and payment systems. For instance, 'false positives' generated by monitoring systems have begun to decrease with this technology, while they also detect more complex laundering patterns. As noted earlier, the use of homomorphic encryption and/or zero-knowledge proof technologies could enable financial institutions to verify certain types of information with each other, without compromising the security or confidentiality of the underlying data.

In addition, the use of digital identification can contribute to a more inclusive financial system which is also more resilient in terms of preventing financial crime, particularly fraud. Leveraging this technology to strengthen the system should be encouraged.

Further work and leadership at the international, regional and domestic level to foster new technologies and review regulatory impediments to innovation will also greatly assist efforts to fight financial crime. The FATF has taken a leading role in leading the global efforts in this area and their continued good work should be fully supported.

Recommendations

The G20 and the broader international community should encourage the process for innovation in financial regulatory technology that assists in compliance with financial crime regulations through examination of key technologies coupled with reform to encourage the use of those technologies where required and where warranted:

Clarify the regulatory stance on adoption of new technology

The promotion of regulatory responses that are clear, actionable, and consistent across jurisdictions is vital in helping accelerate the adoption of new technologies in this area and to assist in increasing systemic effectiveness. In the United States, for example, the Financial Crimes Enforcement Network (FinCEN) and its regulatory partners have issued a joint statement to encourage financial institutions to take innovative approaches to combating money laundering, terrorist financing, and other illicit financial threats.[66] This recognises that private sector innovation, including new ways of using existing tools or adopting new technologies, can help banks identify and report illegal financial activity by enhancing the effectiveness and efficiency of compliance programs. Such an approach should be considered by other jurisdictions through international coordination and must be followed up with effective guidance on which financial institutions can rely.

Creation of local partnerships to test new solutions

Some regulators already run technology 'sprints' supporting the development of innovative approaches to improving financial crime controls.[67] Increasing the frequency, participation and international connectivity in these events will help to accelerate the introduction of enhanced analytics and technology for financial crime. There should also be encouragement for financial institutions to partner and test new technology to help to identify industry sound practices and inform updates to regulatory guidance.

Enhance and expand the use of machine learning for financial crime risk management

The use of machine learning for financial crime risk management can be transformative in enhancing systemic effectiveness and is becoming more widely used. To examine its adoption further, the IIF surveyed a diverse group of banks and insurers on their adoption or exploration of machine learning and artificial intelligence for AML purposes, tapping into regulators' interest in understanding the types of new techniques being pursued to improve AML detection and compliance, as well as enabling these new developments to be shared and better understood across the industry. This is especially pertinent where firms can highlight the barriers or challenges encountered with these technologies and the supporting infrastructure and data feeds, and operational experiences in implementation.

Of the firms surveyed, the application of machine learning techniques in the AML space is spreading quickly across the industry. 35% of participants are already applying them today, in addition to a further 34% percent actively experimenting with them. Another 29% percent are planning to apply these techniques in the foreseeable future. The analysis showed that expected benefits were indeed realised by those who already apply machine learning. The most prominent benefit is an increased speed and/or automation of analysis that allows the AML process to respond to the latest development in money laundering methods. This increase in automation and speed of key process steps will be beneficial to all other process steps built around them. Firms have also reported a reduction of false positive rates and an improved ability to generate alerts that previously remained undetected. Together, these enhanced analytics allow the identification of threats that were unknown previously, again contributing to a stronger defense system.

Despite these benefits, financial institutions remain cautious and are not seeking to replace their staff. The human expert taking a final decision, supported by the enhanced analytical capabilities of the new systems, is the centre of the various initiatives. The results emphasised many of the issues raised in this paper regarding the need for regulatory consistency and enhanced information sharing to improve technological efficiency in the system ,and also spoke to the need for 'explainability' in predictive AI led modelling.[68] Regulators and policymakers should work to examine ways to mitigate the issues for information sharing which inhibit adoption of this new technology and the industry should work to ensure its systems and the quality of its data can support AI techniques for financial crime compliance.[69]

Conclusion

Illicit finance drives and supports some of the worst problems confronting society today, including terrorism, sexual exploitation, modern slavery, wildlife poaching and drug smuggling.

Billions of dollars have been invested in AML/CFT efforts worldwide however, stemming the tide of economic crime remains extremely challenging and the amount of money laundered globally each year is estimated to be 2% to 5% of global GDP, or between 715 billion and 1.87 trillion Euros.

The concepts in the paper build upon the good work currently underway through the Financial Action Task Force (FATF), other public sector bodies and the private sector in tackling this important issue.

Moving forward with the intelligence-led approach outlined in this paper, driven by meaningful reforms to information sharing and reporting frameworks, public and private sector cooperation and the use of technology is essential to improving the effectiveness of the collective response to financial crime, the impacts of which are felt beyond the financial sector and pose a grave threat to society as a whole.

Endnotes

1. Basel Committee on Banking Supervision ("BCBS"), Financial Stability Board ("FSB"), International Organization of Securities Commissions ("IOSCO"), and the International Association of Insurance Supervisors ("IAIS") in this case.
2. United Nations Office on Drugs and Crime ("UNDOC"): https://www.unodc.org/unodc/en/money-laundering/globalization.html
3. Europol (2017) 'From Suspicion to Action: Converting financial intelligence into greater operational impact' p. 4
4. Modern Slavery is also recognised as an overarching global issue, with child exploitation, commercial sexual exploitation and forced labour, and all types of trafficking in human beings as defined through the 2000 Palermo Protocol.
5. Refinitiv (May 2018) 'Revealing the True Cost of Financial Crime: 2018 Survey report, p. 26
6. Illicit financial flows, compiled by the anti-corruption forum – page 5. https://knowledgehub.transparency.org/assets/uploads/kproducts/Topic-Guide-on-Illicit-Financial-Flows_2019.pdf
7. Refinitiv (May 2018) 'Revealing the True Cost of Financial Crime: 2018 Survey report, p. 5
8. Financial Action Taskforce and Asia/Pacific Group on Money Laundering, Financial Flows from Human Trafficking, 2018 www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf
9. Basel Committee on Banking Supervision (September 2012) 'Core Principles for Effective Banking Supervision' pp. 9 – 14
10. In addition to the issues for reform outlined in this paper, consideration should also be given by governments, particularly in emerging economies, to how improving financial literacy and strengthening adherence to the rule of law through reform of the judicial system will assist with financial inclusion and poverty reduction.
11. The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its member jurisdictions. The FATF 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.

    The FATF Recommendations set out a comprehensive and consistent framework of measures that countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. The FATF Recommendations set an international standard, which countries should implement through measures adapted to their particular circumstances. The FATF Standards comprise the Recommendations themselves and their Interpretive Notes, together with the applicable definitions in the Glossary. The areas covered by the FATF Recommendations include: AML/CFT Policies and Coordination; Money Laundering and Confiscation; Terrorist and Proliferation Financing; Prevention Measures (e.g. customer due diligence, suspicious transaction reporting); Transparency and Beneficial Ownership of Legal Persons and Arrangements; Powers and Responsibilities of Competent Authorities and Other Institutional Measures; International Cooperation.
12. We note that many of these conclusions in this paper are consistent with the FATF methodology for assessing effectiveness and are reflected in the conclusions, priority actions and recommendations of FATF mutual evaluation reports, which supports the need for globally coordinated action to be taken on the issues outlined herein.
13. In addition, other international standard setting bodies, including the Basel Committee and the CPMI play a role in shaping financial crime related rules in prudential supervision and in the supervision of payments systems and market infrastructures.
14. We note that in the European Commission's report on its assessment of recent money laundering cases involving EU credit institutions (European Commission, Report on the assessment of recent alleged money laundering cases involving EU credit institutions, July 2019), the lack of effective, proportionate and dissuasive sanctioning powers was recognised as a flaw in the EU-wide framework.
15. There are also examples of the lack of congruity in standards outside of the enforcement area. For instance, the adoption of poorly regulated investment-linked or "Golden" national passport regimes may allow for illicit finance to then find its way into the regulated system.
16. European Commission, Communication: Towards a better implementation of the EU's anti-money laundering and countering the financing of terrorism framework, July 2019
17. The FATF and its nine FATF-Style Regional Bodies (FSRBs) conduct peer reviews on an ongoing basis to assess how effectively their respective members' AML/CFT measures work in practice, and how well they have implemented the technical requirements of the FATF Recommendations. The consolidated assessment ratings covered jurisdictions across EMEA, APAC and the Americas.
18. FATF (September 2019) 'Consolidated assessment ratings'
19. The table collected the results for 76 jurisdictions that were subject to a twofold assessment: (1) an evaluation of the effectiveness of the AML measures against a set of 11 immediate outcomes, which represent key goals that an effective AML/CFT system should achieve; and (2) a technical evaluation reflecting the extent to which a country has implemented the technical requirements of the FATF Recommendations.
20. Out of the 76 jurisdictions evaluated, 39, just over 51%, were found to be non-compliant (indicating major shortcomings) in respect of one or more of the FATF Recommendations.
21. Regulatory coherence is discussed in greater detail in section 6 of this White Paper.
22. For further information see Institute of International Finance (January 2019) Addressing Market Fragmentation: The Need for Enhanced Global Regulatory Cooperation
23. In this regard, we are encouraged by statements by FATF President Xiangmin Liu that the FATF is committed to ensuring that authorities have the tools and expertise to assess new technology in financial services and to promote responsible innovation and that the FATF will hold forums to share expertise between supervisors on good practices in this area: Remarks by FATF President Xiangmin Liu at the Queen Mary – HSBC Annual Lecture on Financial Crime, London, September 10, 2019
24. For example, European Commission recently cited the need for appropriate resources for supervisors and FIUs. However, it notes that in some cases, member state supervisors are critically understaffed (European Commission, Supranational Risk Assessment report, July 2019, p. 15). The FATF has also highlighted deficiencies in FIU staffing in some Mutual Evaluation reports. FIU staffing is discussed in greater detail in section 5 of this paper.
25. http://www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf & http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf
26. https://rusi.org/sites/default/files/20190320_expanding_the_capability_of_financial_information-sharing_partnerships_web.pdf

27. Established in 2014 and launched as an operational pilot in 2015, the JMLIT has provided a mechanism for law enforcement and the financial sector to share information and work more closely together to detect, prevent and disrupt money laundering and wider economic crime. The JMLIT is located in the National Economic Crime Centre.

28. The publication of the UK's Economic Crime Plan represents a significant move in driving forward 'whole-system' responses to economic crime. It builds on the undertakings made in earlier documentations (e.g. the UK's 2016 Anti-Money Laundering and Counter-Terrorist Financing Action Plan, 2017 Anti-Corruption Strategy and 2018 Serious and Organised Crime Strategy), in order to provide a cogent and collective articulation of the action being taken by the public and private sectors to ensure that the UK cannot be abused for economic crime.

29. In Canada, for instance, engagement between Project PROTECT (initially a private sector initiative) and Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) took place at a level of seniority that ensured that private sector participants were aware that both the AML/CFT compliance investigations and FIU priorities of FINTRAC were aligned to the success of Project PROTECT. In Australia, the Fintel Alliance was launched at a high-profile public event, including political and bank leadership, following the development of a detailed set of agreed objectives. This public and high-profile commitment from both public and private sectors is considered important as a demonstration of the partnership approach and a signal that it should receive significant resources and effort from both the public and banking sectors.

30. While the sharing of tactical intelligence between PPPs will drive the most significant outcomes, it is accepted that this kind of sharing is challenging, and inextricably linked to the existence of both trusted bilateral relationships and suitable information sharing gateways which, respectively, take time to build and reform. The same challenges do not exist in relation to the sharing of typologies, and steps should be taken to industrialise the coordinated development and sharing of typologies between PPPs – as noted in further detail in section 3 (Recommendations) of this paper.

    In addition, greater support for PPPs could be considered by the FATF. FATF Recommendations 29 (domestically) and 40.9 to 11 (internationally) set out the activities that FIUs should undertake. Consideration should be given to adding a PPP requirement that could then be considered as a part of the effectiveness assessment for FATF Immediate Outcome 6.

31. De-Risking is a global phenomenon leading to the decline in correspondent banking relationships, which may impact the ability to send and receive international payments, or drive some payment flows underground, with potential adverse consequences on international trade, growth, financial inclusion, as well as the stability and integrity of the financial system. Please see Financial Stability Board, FSB action plan to assess and address the decline in correspondent banking: Progress report, May 2019.

32. In 2017, the IIF published a survey of its members on the legal and regulatory barriers that exist to effective information sharing on financial crime related matters. The survey included 28 individual financial institutions covering information concerning 92 countries across Europe, North America, Asia, Africa, Latin America and the Middle East. At the macro level, the survey found that the vast majority of banks identified restrictions on the ability to share information concerning financial crime related matters as an impediment to effective risk management, and that this issue is indeed global in nature. It also found that some countries are moving in the direction of restricting information exchange even further, which is why urgent, globally coordinated action is critical. The report can be found here: https://www.iif.com/publication/regulatory-report/iif-financial-crime-information-sharing-report

33. Launched in December 2017, the Europol Financial Intelligence Public Private Partnership ('EFIPPP'), currently brings together investigators, regulators and officials from FIUs in seven European nations and the US, as well as senior compliance officers at global lenders with the aim of facilitating the exchange of operational or tactical intelligence associated with on-going investigations, subject to the relevant national legal regimes. The EFIPPP also addresses strategic objectives such as identifying ways in which the regulations relating to information sharing could be enhanced.

34. The Egmont Group is a united body of 164 FIUs that provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing. Notwithstanding the Egmont's Group's efforts, significant challenges remain, notably that counterparty FIUs lack access to the specific information needed by the requesting FIU, and time limitations were not always met.

    There is also the obstacle encountered where the country in which the offence has occurred, or a subject of interest is located, has an FIU that is not an Egmont member or has no FIU at all.

35. It is noted that the Monetary Authority of Singapore ('MAS') recently issued a letter to its banks clarifying their position on this point, making it clear that information should be shared on a group wide basis to prevent financial crime. The UK plans to follow a similar approach too, and while this will be hugely useful step in ensuring that banks are better able to understand fin crime risk internally, it does not address the limitations imposed on information sharing between banks, either domestically or internationally, or the sharing of international information with a local law enforcement body.

    Similarly, as early as January 2011 the Financial Crimes Enforcement Network, administrator of the Bank Secrecy Act (BSA) in the US, clarified the circumstances in which SAR information could be shared with affiliates. The Final Rule and accompanying guidance expanded the ability of certain financial institutions to share SARs, or information that would reveal the existence of a SAR with certain affiliates. The Final Rule explicitly acknowledges that the term 'sharing' within a corporate organisation is distinguishable from a prohibited disclosure, and therefore permits financial institutions to share with affiliates within their corporate organisational structure, provided that the affiliate is itself subject to suspicious activity reporting requirements, under common ownership, and not itself the subject of the SAR. Though the Final Rule stopped short of permitting sharing of SAR information with foreign affiliates (except where the foreign affiliate is the parent entity or head office).

36. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/consolidated-fatf-standard-information-sharing.html .

37. https://www.theguardian.com/world/2017/mar/20/the-global-laundromat-how-did-it-work-and-who-benefited

38. For further practical examples on the size and complexity of the challenge to effective information sharing of AML/CFT information, please see the IIF's fictionalised case study of a global financial institution based on real-life scenarios of a financial crime investigation – the 'Mundus Bank' Example: https://www.iif.com/portals/0/Files/private/32370132_iif_fatf_information_sharing_letter_final_2016.05.25.pdf

39. Specifically, the FATF Recommendations should be updated to take the following changes into account: 1. Countries should ensure that secrecy and privacy laws (such as the EUs GDPR), and tipping-off or similar provisions, do not inhibit the exchange of relevant information, including SARs and associated underlying information, across borders between entities in the same group enterprise; between entities in different group enterprises; and between enterprises and governments, in both directions, for the purpose of managing financial crime risk; 2. Countries should ensure that adequate legal protections for banks sharing information in good faith are in place to facilitate the sharing of information as described above (i.e. 'safe harbors'); 3. Countries should ensure that, where an entity is required to report a suspicion which is based, in whole or part, upon information gathered from outside its own group enterprise or from other jurisdictions, that the applicable laws do not prevent the inclusion of that information in the report which is to be filed; 4. Countries should ensure that, where an entity is required to report a suspicion which relates to activity across a number of group enterprises or a number of jurisdictions, that the applicable laws facilitate the filing of identical reports in each relevant jurisdiction.

40. Specifically, in November 2017, the FATF adopted revisions to the Recommendations to clarify the FATF's requirements on sharing of information and the methodology to assess compliance with the Recommendations. These revisions were helpful in clarifying how assessors and advisors should determine the extent of information sharing at the group-wide level, including with branches and subsidiaries, and whether or not sufficient safeguards are in place to ensure confidentiality and prevent tipping-off.

41. In February 2018, the FATF also adopted revisions to Recommendation 2 on national cooperation and coordination. The amendments expanded the Recommendation to include information sharing between competent authorities and emphasised 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). We believe this change will help improve the compatibility of AML/CFT and DPP rules and will assist in facilitating exchanges of information within the private sector.

42. H.R. 2514, the Coordinating Oversight, Upgrading and Innovating Technology, and Examiner Reform Act (the 'COUNTER Act')is currently pending before congress and is the first major reform of the Bank Secrecy Act, 31 U.S.C. §§ 5311 et seq. ('BSA') and related AML regulations since 2001.

43. European Commission Press Release (1 April 2019) 'Capital Markets Union: Creating a stronger and more integrated European financial supervisory architecture, including on anti-money laundering'. As it is in the banking sector that money-laundering and terrorist financing risks are the most likely to have a systemic impact, AML responsibilities in the financial sector will be entrusted to the EBA to ensure high quality AML supervision and effective coordination among different authorities across all Member States. The new rules seek to strengthen the EBA's role and give to the EBA the necessary tools and resources to ensure effective cooperation and convergence of supervisory standards. Specifically, the EBA has been accorded the remit of ensuring that risks of money laundering and terrorist financing in the Union's financial system are effectively and consistently incorporated into the supervisory strategies and practices of all relevant authorities.

44. European Commission (24 July 2019) 'Report from the Commission to the European Parliament and the Council: Assessing the framework for cooperation between Financial Intelligence Units', pp. 10 – 11. The European Commission Report on recent money laundering cases involving EU financial institutions notes that several member state authorities considered confidentiality requirements prevent efficient cooperation and information exchange between FIUs, law enforcement, prudential and AML/CFT supervisors. Cooperation between Union and third country authorities was also considered challenging, with the Commission citing concern that the transfer of data in certain cases may be in violation of the General Data Protection Regulation ('GDPR').

45. The Common Reporting Standard (CRS) is an information standard for the Automatic Exchange of Information (AEOI) regarding bank accounts on a global level, between tax authorities, which the Organisation for Economic Co-operation and Development (OECD) developed in 2014.

46. The Association of Banks in Singapore (2018), Industry Banking KYC Utility Project After Report – Knowledge Sharing, p 1

47. Financial Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations (updated June 2019), Recommendation 10 (Customer Due Diligence), p 12

48. https://www.bbc.co.uk/news/world-41880153

49. Financial Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations (updated June 2019), Recommendation 24 and 25 (relating to legal persons and legal arrangements, respectively), p 20

50. For example, the introduction of the 'persons with significant control' rule in the UK in 2016, which obliges anyone setting up a company to name the individual who actually owns it, ostensibly sought to eliminate the possibility of the ultimate beneficial owner's identity being obfuscated through an ownerships structure that led beyond the UK to jurisdictions with opaque corporate structures and beneficial ownership disclosure regulations. However, in practice the accuracy and quality of the information supplied by those setting up entities at Companies House is neither checked nor verified. Such an example of poor data policing and governance can give rise to information whose veracity cannot be substantively relied up by financial institutions to meet their KYC obligations at onboarding and ongoing due diligence thereafter.

51. The LEI is a 20-character, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO). It connects to key reference information that enables clear and unique identification of legal entities participating in financial transactions. https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei

52. For further information on MANSA, please see: https://www.mansaafrica.com/wps/portal/AFRIXEM_Portal/Home/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfljo8zifSx9DQyN_Q38DDw9XAwC3X3cTf19jYzd_U30w9EUhBm6GTiaB4QaBgUYGhl4GutHkaYfQwFIvwEO4GhAwP5gAzT7MZwH0Y_HAoL6o_AqAbmAkB8KckNDQyMMMgH54TLZ/dz/d5/L2dBISEvZ0FBIS9nQSEh/

53. The KYC Registry is a global repository of standardised, up-to-date due diligence documents and data. The KYC Registry leverages a community of over 7500 financial institutions with correspondent networks to deliver a single, central repository of information, which SWIFT validates and checks for completeness and accuracy. Correspondents benefit from the ability to add their own data to the KYC Registry so that others can access it, replacing the need to respond individually to each incoming KYC request.

54. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council.

55. For further information on Digital ID, please see: IIF, Digital Identities in Financial Services Part 1: Embedding in AML Frameworks, August 2019: https://www.iif.com/Portals/0/Files/content/Innovation/08272019_iif_digital_id_part_1.pdf

56. Bank Policy Institute, Getting to Effectiveness – Report on US Financial Institution Resources Devoted to BSA/AML and Sanctions Compliance (29 October 2018) p 3. The largest share of resourcing identified in this study was identified as other with 48.6% of AML/BSA compliance staff (this included such elements as personnel engaged in AML/BSA training, development of policies and procedures, quality assurance, and monitoring and testing.
57. Financial Action Task Force, Anti-money laundering and counter-terrorist financing measures: United Kingdom Mutual Evaluation Report (December 2018) p 49
58. Europol (2017) 'From Suspicion to Action: Converting financial intelligence into greater operational impact' pp. 29-31. For the purpose of the report, the conversion rate referred to the way in which a SAR was used, e.g. subject to further analysis, used within the framework of on-going/existing investigations or to launch a new one. The report also highlighted the challenges in any cross-jurisdictional evaluation of SAR conversion rates arising, amongst other things, from the differing remits of the various EU FIUs and methodologies used for recording and analysing information such that calculating a meaningful conversion rate is challenging.
59. For example, a regulator could use a national risk assessment or a collectively agreed threat assessment, to provide banks with an element of guidance on the proportion of resource to be focused on priority threats.
60. We also note that a working group sponsored by the Asian Development Bank (ADB) is currently working on a model to standardise some data elements of the SAR – though not the entire SAR -- across jurisdictions. We believe this initiative, combined with the recommendations contained in this White Paper, should be encouraged in order to enable key data becoming comparable across jurisdictions; facilitate investigations and prosecutions in cross-border trade; facilitate SARs data analysis and identification of trends, particularly in Trade Based Money Laundering (TBML); and develop a better understanding among stakeholders of materiality regarding which data points yield results.
61. For instance, the European Commission recently cited the need for appropriate resources for supervisors and FIUs. However, it notes that in some cases, member state supervisors are critically understaffed (European Commission, Supranational Risk Assessment report, July 2019, p. 15).
62. The issue of KYCC has been addressed through FATF Guidance, however, as noted adoption and understanding of the Guidance is not uniform globally: FATF Guidance, Correspondent Banking Services, October 2016
63. IBID and BCBS, Sound management of risks related to money laundering and financing of terrorism: revisions to correspondent banking annex – final document, June 2017
64. FSB action plan to assess and address the decline in correspondent banking: Progress report to G20 Summit of July 2017, P. 2.
65. In the US for example, testimony submitted by the Office of the Controller of Currency to the US Senate Committee on Banking, Housing, and Urban Affairs in November 2018 highlighted that it had taken the lead in setting up a working group comprising, in addition to itself, other 'federal banking agencies' within FinCEN, which was tasked with looking at promoting innovative and proactive approaches to "identify, detect, and report financial crime, and meet BSA/AML regulatory obligations; and clarify that the agencies do not have a zero-tolerance approach to BSA/AML supervision, but rather employ a risk-based approach to the examination process." Testimony of Grovetta N. Gardineer (Senior Deputy Comptroller for Compliance and Community Affairs – Office Of The Comptroller Of The Currency) Before the Committee on Banking, Housing, and Urban Affairs United States Senate, November 29, 2018
66. Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency; Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing, December 2018.
67. The Financial Conduct Authority in the UK, for instance, regularly holds Global Anti-Money Laundering and Financial Crime 'TechSprints'. The purpose of the TechSprint is to investigate how new technologies and greater international collaboration could help to improve prevention and detection rates for financial crime compliance. https://www.fca.org.uk/events/techsprints/2019-global-aml-and-financial-crime-techsprint
68. For further information on issues for explainability in Machine Learning, please see: IIF, Machine Learning Paper on Explainability in Predictive Modeling, November 2018: https://www.iif.com/Publications/ID/1423/Machine-Learning-Paper-on-Explainability-in-Predictive-Modeling
69. For a full list of recommendations and issues for Machine Learning in AML, please see: https://www.iif.com/publication/regulatory-report/machine-learning-anti-money-laundering

Key contacts – IIF

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 and Head of IIF London Office
+44 (0)20 7006 4149
mekberg@iif.com

Key contacts – Deloitte

Michael Shepard
Principal, Deloitte Risk and Financial Advisory Global Financial Crime Practice leader
+1 215 299 5260
mshepard@deloitte.com

Rob Wainwright
Partner, Deloitte Risk Advisory
+31882885834
rwainwright@deloitte.nl

Katie Jackson
Partner, Deloitte Forensic
+44 (0)20 7303 0586
kjackson@deloitte.co.uk

Tamsin Baumann
Partner, Deloitte Forensic
+44 (0)20 7303 2182
tbaumann@deloitte.co.uk

Chris Bostock
Director, Deloitte Forensic
+44 (0)20 7007 4355
cbostock@deloitte.co.uk

Abu Saleh
Manager, Deloitte
+44 (0)161 455 8055
abusaleh@deloitte.co.uk

Pablo Sapiains Lagos
Manager, Deloitte
+44 (0)20 7007 3754
psapiainslagos@deloitte.co.uk

Deloitte.

Designed and produced by 368 at Deloitte, London. J18737