INSTITUTE of INTERNATIONAL FINANCE

October 2020

Economic and Financial Crime Risk and the Sharing of Intelligence: Updating and Enabling International and Domestic Cooperation in Combatting Illicit Financial Flows

Matthew L. Ekberg, Senior Policy Advisor, Regulatory Affairs, mekberg@iif.com

Research and Review: Michaela Palmer, Program Assistant, Regulatory Affairs, mpalmer@iif.com

INTRODUCTION

It is well documented that the management of economic and financial crime risk can be improved by facilitating the increased sharing of information on financial activity linked to crime and terrorism, both domestically and internationally. Such exchange is important to the proper functioning of Anti-Money Laundering (AML), Countering the Financing of Terrorism (CFT) and other financial crime prevention policies which address key geopolitical priorities well recognized by the international community

Nevertheless, issues such as inconsistent legal frameworks for data protection, the management of Suspicious Activity Report (SAR) type information, privacy, and bank secrecy present barriers that inhibit intelligence sharing. As such, financial institutions, regulators and law enforcement are constrained in seeing the full picture of criminal activity which flows across the global financial system, making the mitigation and eradication of criminal elements much more difficult.

These are not new issues and there continues to be close attention paid to such matters at the international, regional, and domestic levels. Some good progress has also been made in addressing these barriers – in particular by the Financial Action Task Force (FATF). However, with the effects of the COVID-19 pandemic raising novel challenges in relation to financial criminal activity[1], and with numerous financial crime compliance reform efforts under way across the globe, there is fresh opportunity to address a number of factors which prevent the optimum exchange of economic crime data for the genuine purpose of preventing criminal incursion into legitimate financial channels. In order to accomplish this, policy makers should focus attention on three key areas:

> ***First***, at the domestic and regional level, effective implementation of the current FATF Recommendations[2] and guidance which facilitate information sharing should be prioritized. Specifically, changes which were adopted in recent years to FATF Recommendation 2 (cooperation between data protection authorities and AML/CFT author-

[1] For further information on the impact of the COVID-19 crisis on financial crime, please see:

IIF, *Staff Paper: Financial crime risk management and the COVID-19 Pandemic: Issues for closer international cooperation and coordination,* April 2020: https://www.iif.com/Publications/ID/3867/IIF-Staff-Paper-Financial-Crime-Risk-Management-and-the-COVID-19-Pandemic

FATF, *Statement by the FATF President addressing issues concerning COVID-19 and measures to combat illicit financing*, April 1, 2020 and FATF, *COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses*, May 4, 2020

[2] FATF, *The FATF Recommendations*, Updated June 2019

ities and the compatibility of AML/CFT and data protection rules) and the interpretative note to FATF Recommendation 18 (financial institution group-wide information sharing) should be implemented consistently and swiftly across FATF member and associate member jurisdictions with an eye toward ensuring practical and tangible outcomes which improve the ecosystem for exchanging intelligence.

Second, at the international level, the FATF should continue its essential work in this area. The priorities of the two-year German FATF Presidency[3] – and the broader effectiveness objectives of the FATF[4] – should be reviewed in light of how progress can be achieved through potential further updates to the FATF Recommendations and guidance. These updates should help to enable intelligence on economic crime – including SARs and their underlying information – to be shared within financial institutions, between financial institutions, between governments and financial institutions and amongst public sector entities on a cross-border basis. It is important this be done whilst also balancing that exchange with highest standards for data protection, data security and customer privacy. Such continued efforts at the FATF level would benefit international consistency and will be particularly important in advancing efforts to strengthen AML/CFT systems through innovation and the digital transformation.[5]

Third, where national or multilateral reforms to financial crime risk management frameworks are planned or underway, greater information sharing should be a central focus. This includes highly relevant work by the G20 through the international standard setting bodies to enhance cross-border payments[6] – an effort which has the potential for significantly wider benefits to AML/CFT and information sharing reform overall. The G7 and the G20 also have a broader role to play in coordinating amongst member countries to ensure regularity in adoption of reforms.

There is currently a critical opportunity to make meaningful changes in how the global financial community addresses illicit finance. The September 2020 public disclosure of SARs documents filed by financial institutions with the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) – otherwise known as the "FinCEN Files"[7] – underlines what regulators, law enforcement and financial institutions have known for a long time: systemic reform is key to tackling economic crime and at the forefront of that effort should be making intelligence sharing on financial crime risk operative and ultimately beneficial.

BACKGROUND

As has been recognized extensively across both the public and private sectors, the current global framework for fighting financial crime is not as effective as it could be, and more needs to be done at the global, regional and national levels to help identify and stem the flow of illicit finance – an activity which supports some of the worst problems confronting

[3] FATF, *Objectives for the FATF during the German Presidency (2020-2022*), June 2020

[4] FATF, *An effective system to combat money laundering and terrorist financing* :https://www.fatf-gafi.org/publications/mutualevaluations/documents/effectiveness.html

[5] We note the Digital Transformation of AML/CFT is an objective of the FATF Presidency: FATF, *Objectives for the FATF during the German Presidency (2020-2022*), June 2020

[6] Communiqué, G20 Finance Ministers & Central Bank Governors Meeting 22-23 February 2020, Riyadh, Saudi Arabia: *"We recognize the need to enhance global cross-border payment arrangements to facilitate lower-cost and swifter transfers, including for remittances. We ask the FSB, in coordination with the Committee on Payments and Market Infrastructures (CPMI) and other relevant standard-setting bodies and international organizations, to develop a roadmap to enhance global cross-border payment arrangements by October 2020."*

[7] IIF Statement: *Buzzfeed and ICIJ Reports Once Again Emphasize the Need for Reforms*, September 20, 2020: https://www.iif.com/Press/View/ID/4094/Buzzfeed-and-ICIJ-Reports-Once-Again-Emphasize-the-Need-for-Reforms

society today, including terrorism and the proliferation of weapons of mass destruction (WMD), sexual exploitation, modern slavery, fraud, environmental crime and drug smuggling.[8]

Put simply, limitations to information sharing hamper increased effectiveness. These constraints are entirely at odds with the realities of criminal operations, which are not bound by international borders, and indeed actively exploit them to evade civil and criminal penalties. This undermines law enforcement's ability to build a network view of criminal activity and it weakens financial institutions' ability to fully review their exposure to financial crime risk at a global level. The issues are particularly 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, (amongst transactions and counterparties for instance), but the dots cannot be connected. [9]

This national approach to a global problem is not only encountered where financial institutions seek to share intelligence with foreign law enforcement or other institutions, but can even manifest itself within a banking group, where in certain jurisdictional circumstances locally imposed limitations on information sharing prevent data being shared on a group-wide basis.[10] New technology for risk management and compliance in this area will also struggle to reach its full potential if the right, good quality data is unavailable to facilitate machine learning and other activities which can help to achieve better outcomes.[11]

Restrictions to the movement of data across national borders are not new, but they have increased in the last decade in parallel to the development of digital technologies and the associated growth in the storing, processing and sharing of data. On the grounds of law enforcement, national security, personal data protection or economic protectionism, a growing number of jurisdictions have introduced or strengthened different versions of data localization requirements which in many cases stand in contrast to the changes made to the FATF standards over the past number of years.[12]

These issues are well recognized in various international and domestic fora. For example, in the context of the global dialogue on "de-risking"[13], the Committee on Payments and Market Infrastructures (CPMI) has acknowledged that if banks in a correspondent banking relationship cannot provide additional information on customers and specific transactions due to legal and regulatory restrictions on information exchange, correspondent banks may have no alternative but to block or reject certain transactions. This may in some cases lead to the termination of some banking relationships and contribute to financial exclusion.[14] More recently, the Bank for International Settlements (BIS) indicated that information-sharing

[8] For further information on these issues, please also see: IIF/Deloitte, *The Global Framework for Fighting Financial Crime: Enhancing Effectiveness and Improving Outcomes,* October 2019*:* https://www.iif.com/Publications/ID/3606/The-Global-Framework-for-Fighting-Financial-Crime-Enhancing-Effectiveness-Improving-Outcomes

[9] There are also many interconnected issues for accessing information. A lack of transparency in beneficial ownership information is one area of concern. Another can be the access to information related to parties charged or even convicted of predicate offenses. Although this may be a sporadic issue as some countries have this information available in open databases, it is inconsistent and a challenge for most reporting entities to do a look-back view of crime which may have already happened in their existing databases.

[10] IBID, Pp. 15-20.

[11] IIF, *Machine Learning in Anti-Money Laundering*, October 2018: https://www.iif.com/Publications/ID/1421/Machine-Learning-in-Anti-Money-Laundering

[12] IIF, *Data Flows Across Borders*, March 2019: https://www.iif.com/Publications/ID/3283/Data-Flows-Across-Borders

[13] The term "de-risking" has become common shorthand for referring to any instances in which banks have adopted increasingly stringent financial crime-related policies to reduce their exposure to potential money laundering, terrorist financing, corruption or sanctions risk. More specifically, it relates to the strategies adopted by banks to reduce or eliminate their risk exposure. The term tends to be used particularly where multiple businesses in a given category or country are affected.

[14] CPMI, *Correspondent Banking*, July 2016.

initiatives between financial institutions, as well as between jurisdictions, offer opportunities for reducing cross-border frictions in this area.[15]

The CPMI also addressed issues for information sharing reform in the context of enhancing cross-border payments.[16] The CPMI has reported to the G-20 that the sharing of information across borders is required for supervision and oversight as well as more effective risk management. However, in some cases, there can be friction – real or perceived – between regulatory requirements, including banking regulation and AML/CFT rules, on the one hand, and restrictions on cross-border data flows and data storage, on the other.

The Financial Stability Institute (FSI) has likewise noted the need for authorities to review and balance the objectives of data privacy vis-a-vis financial transparency as well as the need to review information-sharing frameworks to identify or establish appropriate legal gateways for exchanging data. The FSI emphasizes that this should be developed in the context that improved cooperation can help to reduce unwarranted de-risking, which would further aid in enhancing financial inclusion, especially in emerging markets.[17]

The Financial Stability Board (FSB) has further observed that issues concerning data localization can lead to greater market fragmentation. They specifically noted that significant differences in data reporting requirements and obstacles to information sharing across jurisdictions can increase the compliance cost associated with financial institutions' cross-border operations. In the extreme, this can cause firms to withdraw from certain activities, impair data quality, usability and ease of aggregation in ways that hinder authorities' ability to analyze global data sets.[18]

As discussed further in section one of this paper, the FATF has been a leader in this area and has emphasized that it is crucial for information concerning financial activity with possible links to crime and terrorism to be shared in a timely and effective manner between and with both the public and private sector. They have highlighted that information sharing can allow financial institutions, supervisory and law enforcement authorities to make better use of available resources and exploit new technologies and business models to develop innovative techniques to tackle money laundering and terrorist financing.[19] In the context of the COVID-19 crisis, the FATF further stressed that public/private cooperation on information exchange is particularly important in tackling new and emerging risks.[20]

Though there is certainly an ever-expanding consensus on these issues and some progress has been made in efforts to facilitate greater information exchange, it is important to address these matters holistically in several key ways.

RECOMMENDATIONS

1. Implementation of Updated FATF Standards on Information Sharing – Recommendation 2 and the Interpretative Note to Recommendation 18

As noted, the FATF has been forthright in the need for greater information exchange as a means to tackle financial crime and several extremely positive developments have emanated from their essential work. First, under the Argentinian FATF

[15] Bank for International Settlements, *On the Retreat of Correspondent Banks*, March 2020.

[16] CPMI, *Enhancing cross-border payments: building blocks of a global roadmap*, July 2020.

[17] FSI, *Closing the loop: AML/CFT supervision of correspondent banking*, September 2020.

[18] FSB, *Updates on the Work on Market Fragmentation*, October 2019. We also note the FSB has prioritized international cooperation and the sharing of information in the broader policy response to the COVID-19 crisis: https://www.fsb.org/work-of-the-fsb/addressing-financial-stability-risks-of-covid-19/

[19] FATF, *Guidance on private sector information sharing*, November 2017.

[20] We note the FATF has stated that supervisors, financial intelligence units and law enforcement agencies should continue to share information with the private sector to prioritize and address key ML risks, particularly those related to fraud, and TF risks linked to COVID-19: FATF, *FATF COVID-19 Statement*, April 1, 2020.

presidency, important strides were made in offering both guidance and updating the FATF Recommendations[21] in this area. In November 2017, the FATF adopted revisions concerning the interpretative note to Recommendation 18 clarifying how assessors and advisors should determine the extent of sharing of information at group-wide level, including with branches and subsidiaries, and the whether or not sufficient safeguards are in place to ensure confidentiality and prevent tipping-off.[22] The FATF also published important formal Guidance on information sharing more generally which sets out the requirements of the FATF Recommendations in this area. [23]

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 emphasized that cooperation should include coordination with the relevant authorities to ensure the compatibility of AML/CFT requirements with Data Protection and Privacy (DPP) secrecy rules and other similar provisions (*e.g.,* data security / localization).[24]

The updates to Recommendation 2 are particularly important, especially when considering the changes underway in the digitization of financial services and the need to ensure data is available to drive forward effective innovation. Once enacted jurisdictionally, this change will help to make sure AML/CFT and DPP rules are accordant and will assist in facilitating exchange of information within the private sector. Data protection, data security, data privacy and the ethics of data remain critical when dealing with the concept of sharing information. Whilst the protection of customer/personal data and the right to privacy are of unquestioned importance, the upholding of such principles is not mutually exclusive with sharing information on illicit financial activity in a safe and secure way where necessary to limit its furtherance.

The CPMI has raised issues regarding tensions between data protection and information sharing in their report on enhancements to cross-border payments. They found that there is in some cases real or perceived friction between information sharing and rules related to data protection, privacy and confidentiality that may restrict or prohibit information-sharing. [25] The CPMI has also stated that limited cooperation among financial regulatory and supervisory bodies on these issues, as well as with data protection and privacy agencies, can exacerbate these possible tensions.[26]

As such, national adoption of changes to the updated FATF standards will greatly assist in alleviating some of these issues in order to find legal gateways for exchanging intelligence. As these changes are relatively recent, there is currently a limited number of completed assessments on implementation for the FATF to consider overall compliance. Nevertheless, according to FATF data, of the ten jurisdictions assessed by FATF against the new criterion for group-wide information sharing under the Recommendation 18 interpretive note changes, two have fully met the criterion, four have largely met it, and four partly met it. Some jurisdictions in particular, including the United Kingdom and Singapore for example, have

[21] FATF, *The FATF Recommendations*, Updated June 2019.

[22] FATF, *Outcomes Joint FATF/GAFILAT Plenary, 1-3 November 2017.*

[23] FATF, *Guidance - Private Sector Information Sharing*, November 2017.

[24] FATF, *Outcomes FATF Plenary, 21-23 February 2018.*

[25] Similar issues were found in the IIF research on legal and regulatory barriers to information sharing, whereby internal policies at financial institutions can restrict information sharing. While this is not surprising, it calls into question whether a form of information sharing may be possible in law in a specific jurisdiction, but still might not be within a bank's own risk appetite. In some respects, banks' judgments behind such policies may reflect ambiguities or questions about legal requirements or risks. IIF, *Financial Crime Information Sharing Survey Repor*t, February 2017: https://www.iif.com/publication/regulatory-report/iif-financial-crime-information-sharing-report

[26] CPMI, *Enhancing cross-border payments: building blocks of a global roadmap*, July 2020.

produced effective guidance in this context.[27] However, there are still obvious limitations in global action and adoption which call for improvement.

For Recommendation 2, analysis of the FATF Mutual Evaluation Reports (MER) since adoption of the outlined changes reflect action in line with the scope of supervisory cooperation envisioned – with thirty-six jurisdictions assessed under the applicable criteria[28] having a level of compliance in place.

However, such an evaluation of compliance does not always fully reflect whether the Recommendation 2 changes have been effective in what we believe should be their ultimate goal – de-conflicting laws and regulations in relation to AML/CFT and data privacy. Many of the evaluations indicate a level of supervisory cooperation between the relevant authorities, however, there should be further focus on whether the outcomes of that cooperation have led to changes or clarifications in laws/regulations and material growth in gateways to data exchange. This will be the ultimate test as to whether the Recommendation changes actually support real progress.

As such, we believe countries should act quickly in adopting and activating these FATF changes and the FATF itself should continue to rigorously review their national adoption through criteria which reviews efficacy in line with the FATF's overall objectives. The utility of any Recommendation change is only as good as both its practical application in national rule-books/guidance *and* its actual, measurable results in line with both the letter and spirit of the revisions. We also believe benchmarking the adoption of the FATF guidance on information sharing[29] should be prioritized. Understanding how FATF jurisdictions are applying the guidance and how effective that guidance is for improving the environment for information exchange is vital.

2. Prioritization of Information Sharing Reform in Relation to the FATF Objectives

As Germany assumes the first two-year presidency of the FATF, we note the close alignment of the private and public sector goals to counter money laundering and migrant smuggling, environmental crime, illicit arms trafficking and the financing of ethnically or racially motivated terrorism.[30] Upcoming work on the digital transformation of AML/CFT will also be of particular importance. Financial institutions are increasingly using sophisticated tools to manage these risks – and provide information to law enforcement which is "investigation ready" – with technology and data analytics at the heart of the solutions.

We encourage the FATF to examine the interconnectedness of information sharing gateways and barriers as a prism through which to view progress in these critical areas. For example, improving the understanding in the international community of financial flows and cross border linkages between terror groups and individuals, along with their means and donor structures, will require close public and private sector cooperation on sharing the tactical data which underpins this activity. A new FATF initiative focused on financial flows, money laundering and terrorist financing linked to migrant smuggling networks and their transnational routes must take into account evolving data related to the COVID-19 pandemic and shifts in these flows and routes necessitated by border closures. Being able to exchange and analyze the actual data on an international basis will be more effective than relying purely on strategic level exchanges through typologies and geographic indictors.

---

[27] HM Treasury, *Government statement on cross-border information-sharing within corporate groups*, May 2020 and Monetary Authority of Singapore, *FATF Guidance on Private Sector Information Sharing and Revised INR.18*, March 2018.

[28] FATF, Criterion 2.5: *To ensure the compatibility of AML/CFT requirements with rules on data protection and confidentiality and to promote the exchange of information by competent authorities*. Analysis reflects where an MER has specifically addressed Criterion 2.5 since March 2018.

[29] FATF, *Guidance - Private Sector Information Sharing*, November 2017.

[30] FATF, *Objectives for the FATF during the German Presidency (2020-2022)*, June 2020.

The digital transformation of financial crime risk management will present some of the strongest opportunities to incorporate standards for improved information sharing in order to achieve better outcomes. This becomes even more relevant as the COVID-19 crisis has moved more and more business activity online.[31] As the FATF undertakes a study of opportunities and challenges of new technology in order to make the implementation of AML/CFT measures by the private sector and supervisors more efficient, we encourage the FATF to consider the limitations imposed on new types of technology without better data exchange opportunities.[32]

For instance, machine learning for AML/CFT risk management holds great promise; however, one of the biggest challenges to its increased use is data sharing impediments along with poor data quality. Building the high-quality datasets required to make the most of the new technology including machine learning algorithms is difficult under conditions where the access to data is restricted. Financial institutions can only rely on their information to identify which alerts should be flagged in the future, but not on the outcome to fine tune their models or the broader data set available due in part to the localization of information sharing rules. This applies especially in the case of data protection issues. It becomes difficult for financial institutions to navigate an area of data analysis in which a regulator would consider that it has applied an appropriate level of care in its safeguards without overstepping on the privacy rights of its customers or other affected third parties.[33]

We also note that there is scope for further examination of technologies which may directly address information sharing and data privacy concerns. A closer review of how privacy preserving or enhancing technologies which contribute to a system that enables the flow of relevant data is also warranted, in addition to addressing the structural and legal issues involved with operational information sharing.[34]

Beyond the formal priorities of the current Presidency, there is likewise opportunity to achieve the wider aims of the FATF with a focus on the exchange of financial intelligence. For example, these issues are particularly important in the context of FATF's work on updates to FATF Recommendation 1 and its Interpretive Note, which seeks to mitigate proliferation finance risk and the consequences which flow from the potential breach, non-implementation or evasion of targeted financial sanctions obligations.[35] Actionable information sharing, however, is the only truly effective way for financial institutions to address proliferation financing risks and concomitant data sharing reform would have measurable effects in preventing the financing of the proliferation of WMDs, including chemical, biological and nuclear weapons. [36]

Notwithstanding the progress already addressed in section one of this paper, it is clear that an operative means of ensuring FATF members review and adapt/clarify their national laws and regulations to improve information sharing (particularly the underlying operational and tactical data) will be essential to help achieve the FATF Presidency priorities and the wider

[31] We note that the FATF has stated that in line with the FATF Standards, it encourages the use of technology, including Fintech, Regtech and Suptech to the fullest extent possible. It also notes that digital/contactless payments and digital onboarding reduce the risk of spreading the virus: FATF, *FATF COVID-19 Statement*, April 1, 2020.

[32] We recognize that information sharing and better data frameworks are not the only issues that will increase effectiveness and efficiency in the use of technology in this area. For instance, some uncertainty remains regarding the support of regulators for this technology as part of an adequate risk mitigation framework. The IIF recommends a stronger statement of support for the application of new technologies in the prevention of money laundering and financial crime, as well as a cooperative approach between public and private sector to determine best practices for the methodology in this context. For further analysis of recommendations on technology and financial crime risk management, please see: IIF, *Machine Learning in Anti-Money Laundering*, October 2018 for Machine Learning and IIF, *Digital IDs in Financial Services Part 1: Embedding in AML Frameworks*, August 2019 for Digital Identity.

[33] IIF, *Machine Learning in Anti-Money Laundering*, October 2018: https://www.iif.com/Publications/ID/1421/Machine-Learning-in-Anti-Money-Laundering .

[34] For further information, please see: RUSI/FFIS, FFIS Privacy Enhancing Technology Project: https://www.future-fis.com/the-pet-project.html.

[35] FATF, Public Consultation on FATF's Recommendation 1 and its Interpretive Note, June 2020.

[36] IIF/Wolfsberg Group, RE: Public Consultation on FATF's Recommendation 1 and its Interpretive Note, September 2020: https://www.iif.com/Publications/ID/4073/IIF-Responds-to-FATF-CP-on-Proliferation-Finance-and-Sanctions-Obligations.

goals of the FATF, especially when viewed through the scope of effectiveness of the FATF standards across the globe.[37] As such, further updates to FATF standards and guidance which would enable intelligence on economic crime to be shared within financial institutions, between financial institutions, between governments and financial institutions and amongst public sector entities on a cross-border basis should be considered as part of the overall efforts to ensure consistent progress is achieved internationally in all these areas.

The FATF should also continue to actively support the creation of public/private partnerships (PPP) as a means to advance information sharing goals. At the center of an intelligence-led financial crime mitigation model is the PPP – a collaboration between financial institutions, law enforcement 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 catalyze coherent reform of the wider financial crime risk management framework.

Many of the same challenges on information sharing gateways can exist for PPPs, however they are an effective tool for addressing risk in this area and should be considered as essential in the wider context of fulfilling domestic and international anti-financial crime objectives.[38] Where there is statutory underpinning for PPP data sharing, this can also expedite overcoming some of the impediments outlined herein. In addition, more established PPPs are beginning to explore what new technologies can be used to enable more effective information sharing, including privacy enhancing technologies.

3. Incorporating Information Sharing Enablers into Domestic and Multilateral Reform Efforts

There are currently a number of efforts underway at the global, regional and national levels to modernize financial crime risk management frameworks through updates to domestic or multilateral regimes and opportunities should be taken to address a number of the issues and challenges outlined in this paper, including implementation of FATF Recommendation 2 and 18 updates as laid out in section one herein.

In the European Union (EU), for example, the European Commission has produced an action plan for a comprehensive EU policy on preventing money laundering and terrorist financing.[39] The proposals in the plan hold a great deal of promise for strengthening and harmonizing EU AML/CFT rules across the EU and addressing shortcomings in those rules. In particular, the Commission has expressed support for PPPs as a means to better enable an intelligence-led approach in these areas. This work should be encouraged, and the Commission should also adopt provisions which allow for the sharing of critical financial crime data – including SARs and associated underlying information – in circumstances where it is currently not possible. [40]

In the United States, the 2020 National Strategy for Combating Terrorist and Other Illicit Financing also advocates for the greater use of PPPs and improved cross-border and domestic information sharing whilst acknowledging that there are overly restrictive laws and regulations which prevent successful exchange of information.[41] Action on the issues raised in

[37] FATF, *An effective system to combat money laundering and terrorist financing* :https://www.fatf-gafi.org/publications/mutualevaluations/documents/effectiveness.html.

[38] For further information on the status of public/private partnerships, please see: RUSI/FFIS, *Five Years of Growth of Public-Private Partnerships to Fight Financial Crime*, August 2020: https://www.future-fis.com/thought-leadership-in-partnership-development.html

[39] European Commission, *COMMUNICATION FROM THE COMMISSION on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing*, 7 May 2020.

[40] IIF, *RE: COMMUNICATION FROM THE COMMISSION on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing*, August 2020: https://www.iif.com/Publications/ID/4055/IIF-Letter-on-EU-AMLCFT-Action-Plan .

[41] United State Department of the Treasury, *National Strategy for Combatting Terrorist and Other Illicit Financing*, 2020.

the strategy coupled with US Congressional action in areas like beneficial ownership information reform will greatly improve the environment for combatting illicit finance both domestically and in partnership with other countries.[42]

We also note that FinCEN has recently outlined options intended to provide financial institutions greater flexibility in the allocation of resources and greater alignment of priorities across industry and government with the intention of enhancing effectiveness and efficiency of AML programs. [43] This is another area where some of the deficiencies in enabling an intelligence-led financial crime model can be addressed.

In the United Kingdom, the government's Economic Crime Plan[44] is a joint public/private blueprint for reforming the country's framework to tackle financial crime, and it has information sharing as a core part of the reforms. Building on the changes made in the Criminal Finances Act 2016, the plan looks to advance information sharing further.

In Singapore, a national AML Blueprint which includes enabling the sharing of data between financial institutions, including the development of a set of risk triggers to initiate such an exchange, has been developed. With the support of legislative changes, this initiative has real potential to improve the environment for targeted financial crime risk management.

The international standard setting bodies are also examining these areas closely and global efforts should especially be encouraged to enable consistency in overall approaches, in close coordination and alignment with the FATF. The Basel Committee on Banking Supervision (BCBS) for instance has recently amended its overall guidance on *Sound management of risks related to money laundering and financing of terrorism*, enabling greater interaction, cooperation and information exchange between AML/CFT and prudential supervisory authorities.[45] This globally consistent guidance will assist in filling gaps in this area, including in relation to mechanisms which facilitate such cooperation in the jurisdictional and international context.

It should be a priority of member states of the BCBS and beyond to consistently implement this guidance domestically and/or regionally and the BCBS should enable a means of benchmarking that reform and its effectiveness. Simply having cooperation mechanisms in place does not help without tangible deliverables which obviate the problems the guidance is ultimately trying to address, including conflicts of laws and practices which inhibit an effectual anti-financial crime regime – particularly across jurisdictions.

As noted earlier, the CPMI has also addressed AML/CFT and information sharing issues as part of its report on enhancing cross-border payments. The report is stage two of an effort by the G-20 and coordinated by the FSB to enable "faster, cheaper, more transparent, and more inclusive cross-border payment services."[46] As part of the "building blocks" set out in the report on how payment system enhancements could be achieved, the CPMI considers issues for applying AML/CFT rules consistently internationally, fostering know-your-customer (KYC) and identity information-sharing and, in conjunction with AML/CFT requirements, reviewing the interaction between data frameworks and data protection. The CPMI correctly states that difficulties in these areas can arise from underlying legal frameworks and that there are challenges coordinating and securing support for alignment with international rules and standards and cooperative supervision and oversight arrangements.

---

[42] US House of Representatives: *Bipartisan Corporate Transparency Act,* 2019 and US Senate: *Illicit CASH Act*, 2019.

[43] FinCEN, *ANPR: Anti-Money Laundering Program Effectiveness*, September 2020.

[44] HM Government/UK Finance: Economic crime plan 2019 to 2022.

[45] BCBS, *Sound management of risks related to money laundering and financing of terrorism: revisions to supervisory cooperation,* July 2020 and IIF, *Re: Introduction of guidelines on interaction and cooperation between prudential and AML/CFT supervision*, February 2020: https://www.iif.com/Publications/ID/3752/IIF-Letter-on-BCBS-AMLCFT-and-Prudential-Supervision-Consultation.

[46] CPMI, *Enhancing cross-border payments: building blocks of a global roadmap*, July 2020.

This effort holds great promise in not only enhancing cross-border payments but also addressing structural drivers to de-risking and positively impacting many of the ancillary issues which prevent a fully effective global anti-financial crime framework.

As the G20 and the international standard setting bodies continue this project, recommendations which support enhanced regional and international cooperation in AML/CFT supervisory matters and the development and implementation of technologically innovative solutions for AML/CFT compliance and compliance monitoring should be considered. Further work should be done on analyzing and addressing constraints on cross-border data-sharing imposed by existing national/regional data frameworks, in coordination with the private sector.[47]

Most importantly, the adaptation of data-sharing rules of supervisory and oversight standards to facilitate cross-border exchange of data and information-sharing should be addressed holistically on an international basis, as noted in section two herein.[48]

Lastly, the G20 and the G7 also have a role to play more broadly in coordinating the efforts at reform across jurisdictions. By driving a platform for consistency in adoption of international standards – coupled with actively aligned reforms prioritizing an intelligence-led approach to financial crime risk management through information sharing – progress can be made in a coherent fashion for institutions, regulators and law enforcement aiming to address risk on a cross-border basis.

CONCLUSION

Data localization and barriers to the cross-border exchange of relevant financial crime information remain a significant impediment to building a better anti-financial crime framework on a global basis. These issues are not new, and some good progress has been made in addressing them. However, there is currently significant opportunity to benefit from reforms put in place by the FATF and to capitalize on potential restructuring efforts at the global, regional, and national levels. This becomes even more important given the changing threat landscape as a result of COVID-19. A more effective system for tackling illicit finance – especially one supported by innovation and technology – starts with the building blocks of critical strategic and operational intelligence utilized by both the public and private sectors in a secure way which upholds data security and privacy protections.

In order to do this, we encourage consideration of the three elements outlined in this paper. By consistently/effectually implementing current international standards on information sharing facilitation, focusing on further data sharing improvements through the FATF and actively pursuing global, regional and domestic reform in a coordinated fashion, there is potential for real progress in what should be the ultimate goal of financial crime information sharing – leveraging the combined powers of the public and private sector to curtail illicit flows.

[47] 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. We have 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 IIF would be pleased to consider updating this survey in line with the work of the FSB in this area. The report can be found here: https://www.iif.com/publication/regulatory-report/iif-financial-crime-information-sharing-report.

[48] These areas are all areas raised by the CPMI in Stage 2 of their report to the G-20. The IIF stands ready to work with the FSB and the CPMI as and when these issues may be taken forward.