January 14, 2022

By electronic submission to fsb@fsb.org

Mr Kieran Murphy
Secretariat to the Financial Stability Board
Bank for International Settlements, Basel

Dear Mr. Murphy,

FSB request for written feedback on data frameworks affecting cross-border payments - your response welcome by 14 January 2022

Thank you for your request of 3 December 2021 seeking the IIF's input on how requirements applicable to data could affect cross-border payments by potentially affecting cost, speed, access, security of cross-border payments, or interoperability of cross-border payment networks, and seeking our views on potential frictions, as well as which policies are most effective. We also note the questions and background information attached to your request were published on the FSB's website. We have drawn them to the attention of our members, some of whom you have also contacted directly.

In this response, we largely limit ourselves to general observations and conclusions, building on relevant work of the IIF over recent years, that we hope may be helpful to the FSB in framing and guiding its very valuable work in progressing Building Block 6 of the G20's cross-border payments roadmap (**Roadmap**). In **Annex 1**, we draw tentative conclusions from this work in answer to your detailed questions. In **Annex 2**, we provide further background to these general remarks. In the time available, we have not sought to undertake a full member data gathering exercise, although our members have had the opportunity to review this submission and have provided input.

Digital economic cooperation and the costs of data localization

The topic of data barriers and data localization is one that has risen to the top of the IIF's digital finance agenda, with the recent publication of our Strategic Framework for Digital Economic Cooperation (Oct. 2021).

As we state in this staff paper, which is soon to be followed by a further paper containing recommendations, many governments have been limiting market access for digital products and services, restricting data transfers, forcing foreign companies to invest in duplicate data centres in-country, and invoking protectionist barriers on digital designs. Digital localization also blocks many of the benefits and innovations of public cloud-based solutions and services.

From the IIF's perspective, fundamentally data localization interferes with the principle that data's value is maximized when it can flow with trust and permission across companies, sectors, and national borders to be used.[1] Data localization requirements that prevent the flow of data, or render that flow more expensive, therefore involve an impairment in value that would otherwise be present.

Beyond the direct costs within the financial services industry, the impacts transmitted across the entire economy include weakened systems, reduced connections to global value chains, and less opportunity to leverage global data and technology resources in areas including fraud prevention and efficient payments. [2]

[1] IIF (2021), Strategic Framework for Digital Economic Cooperation (October), pp. 2-3
[2] IIF (2021), *op. cit.*, p. 11

In fact, financial institutions (**FIs**) we asked about regulatory pain points in framing our recent report on Cloud Adoption and Regulation in Asia-Pacific Financial Services (Nov. 2021) tended to revert to the topic of data localization. These measures can take three broad forms:

- conditional limitations on data export (for example, on personal identifying information);
- **local copy or processing requirements**, i.e. the requirement to maintain a local copy of or process a particular data set in jurisdiction;
- "hard" localization, i.e. outright **prohibitions on data export**, or where export is only permitted under very challenging conditions (such as individual regulator approvals).

A fourth type of data barrier can arise from **regulatory fragmentation** (e.g., in implementation of KYC and AML rules) or **inconsistent implementation** of international payment message standards and the data required to be included within payment messages.

Data frameworks and AML/CFT related issues; prior FSB work

Data frameworks can interact and sometimes conflict with information needs in the cross-border payment context. This is particularly acute with the flow of information concerning financial crime matters, where cross-border friction can negatively impact the inherently multi-jurisdictional nature of the international payments market. As the CPMI has reported to the G20, difficulties in this area can arise from underlying legal frameworks and there are challenges coordinating and securing support for alignment with international rules and standards and cooperative supervision and oversight arrangements.[3]

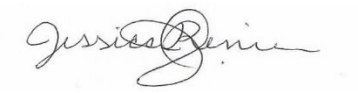
Addressing these issues through a coordinated international effort would benefit the global payments ecosystem and also improve the wider approach to tackling illicit financial flows. Put simply, limitations to information sharing hamper increased effectiveness. These constraints are at odds with the 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 FIs' ability to fully review their exposure to financial crime risk at an international level.

The IIF would also recall that the FSB has undertaken detailed work on data barriers in the context of OTC derivatives data sharing that may be quite informative to the present work.[4]

Conclusion

The IIF thanks the FSB for this opportunity to provide input to the policy development process and stands ready to engage in any stakeholder engagement process or interactive implementation process that is desired. Please feel free to contact me, Conan French or Laurence White with any query.

Yours sincerely,



Jessica Renier
Managing Director, Digital Finance

[3] CPMI (2020), Enhancing cross-border payments: building blocks of a global roadmap.
[4] See FSB (2018), Trade reporting legal barriers: Follow-up of 2015 peer review recommendations. More detail is given in the Annex.

Annex 1

Observations on FSB's detailed questions

1. **How, in your view, do data-specific requirements or objectives of existing national and regional data frameworks, such as those listed above, currently affect (either positively or negatively):**

    a. **the cost and speed of delivering payments,**

Broadly speaking, data localization measures and other data barriers (**Data Barriers**) increase the cost and reduce the speed of cross-border payments, while also increasing operational risk.

Data Barriers arising from data localization typically take three broad forms:

- conditional **limitations on data export** (for example, on personal identifying information);[5]
- **local copy or processing requirements**, i.e. the requirement to maintain a local copy of a particular data set in jurisdiction, or to process the data set in the jurisdiction;
- "hard" localization, i.e. outright **prohibitions on data export**, or where export is only permitted under very challenging conditions (such as individual regulator approvals).

A fourth type of Data Barrier can arise from **regulatory fragmentation** (e.g., in implementation of KYC and AML rules) or **inconsistent implementation** of international payment message standards and the data required to be included within payment messages, including the potential for Payment Service Providers (**PSPs**) to interpret country requirements on an individual basis. This fourth type of Data Barrier, particularly when combined with data localization measures, can make it especially challenging to effectively manage risk related to payments, by making it difficult to undertake customer due diligence on a cross-border basis, and consequently to detect fraud and financial crime. The fragmentation of data formats also exacerbates – and in some ways replicates – the impact of data localization measures by requiring unique onshore processes and systems for compliance or execution purposes.

The means whereby Data Barriers increase cost and reduce the speed of cross-border payments, while increasing operational risk, include:

- reducing or eliminating the scope for data aggregation, and therefore limiting the ability to accurately model global risk, limiting the effectiveness of anti-fraud or AML systems, and complicating the use of global screening and monitoring systems that allow legitimate payments to go through in a timely manner;
- the cost of duplication of infrastructure or operations due to data localization measures;
- limiting the economies of scale that would otherwise be reaped from cloud solutions;
- increasing cyber risk by increasing the attack surface and entry points for cyber-attacks; and
- increasing the risk of, or the complexity and assessment of incomplete or irrelevant payment information leading to, payment fails or manual processing.

[5] For example, where personal identifying information may only be exported subject to appropriate relevant controls, or client confidential information may not be exported without client consent.

Data Barriers can also reduce the effectiveness of supervision, particularly around cross-border payments or institutions.

b. access and transparency (e.g., through compliance costs or through measures enabling or reducing competition) and

To the extent that compliance costs and operational risks are increased by Data Barriers, this may reduce competition by leading to some market actors exiting particular jurisdictions or payment corridors.

Many global FIs rely on cross-border data flows to give local clients access to global platforms. Measures that inhibit cross-border data flows can impact this connectivity and access, or create effective barriers to entry. When jurisdictions encourage or mandate the use of domestic gateways, this can make it more challenging for smaller players to connect with markets and customers outside the local system. Related costs of implementation and compliance are generally passed on to local consumers and clients, working against the policy goal of reducing the cost of cross-border payments.

Transparency measures may also be made more difficult by Data Barriers, for example if there are issues with reporting fees or charges incurred in the payee's jurisdiction back to the paying jurisdiction. Also, if transparency information shared between parties is not included in the payment message in a standardised way, systems will not be able to present the information in a consistent way to payers or payees.

c. other aspects that affect the delivery of, or regulatory compliance with respect to, cross-border payments?

Data Barriers, as stated above, may reduce or eliminate the scope for data aggregation, and therefore limit the ability to accurately model global risk, and limit the effectiveness of anti-fraud or AML systems.

2. More specifically, what barriers to cross-border use of data do you see in existing data frameworks that will impede our ability to address the four challenges faced by cross-border payments?

Global platforms that store and consume data including individual or entity-level data can enable faster and cheaper cross-border payments.

Personal data regimes that block the transfer of data into certain jurisdictions (e.g., in the absence of equivalent or adequate regulatory protections) can make it operationally complex if not impossible to execute cross-border payments through these global platforms by requiring duplication of systems and processes and/or workarounds. This is particularly the case where client consent cannot be obtained to transfer of that data in that way.

Local copy or processing requirements to store and/or process certain data onshore, including data necessary for payments transactions, can also limit the use of cost-effective, secure, and reliable global systems, including those that operate in the cloud.

Fragmentation and inconsistent implementation create barriers to consistency in payment messaging which have the potential to negatively impact each of the four challenges faced by cross border payments by inducing friction into the end-to-end payment process.

Friction in the payment process due to inconsistencies in payment messages increases operational costs and decreases speed, as payments fail, or require manual intervention, more frequently. Transparency targets are also impacted as requisite information is not available to share with customers. Furthermore, in the event that data quality is sufficiently poor in a particular country, PSPs may choose not to provide services, limiting access to customers.

Currently, examples of such barriers include country-specific interpretations of FATF AML/CFT payment messaging requirements. Today, there are varying interpretations of the mandatory payment message fields and text format required to satisfy the FATF guidelines.

In the future, there is the potential for ISO 20022 formatted messages to support richer data, but differences around the free format field, or the status of the mandatory fields, may result in added complexity, impacting the determination of missing or incomplete information.

Providing greater standardization and conformity for payment message information would reduce or remove existing friction in the end-to-end cross border payments process, positively impacting all four of the challenges.

3. **What areas of improvement could you suggest in data frameworks in order to overcome these barriers? Are there effective practices you would highlight to the FSB membership?**

Provision of standardized gateways

Consideration should be given to setting out standardized gateways or exceptions to Data Barriers, clarifying the circumstances under which authorities and FIs may make disclosures despite the presence of a Data Barrier.

There are distinct levels of Data Barrier that may be relevant and should be considered and addressed separately:

- B2B: Data flows between different private sector entities, within or without corporate groups;
- B2G/G2B: Data flows between private sector entities and official sector authorities;
- G2G: Data flows between official sector authorities.

For example, **B2B and B2G barriers** arising from data localization measures could be addressed by providing a **"gateway"** or exception to facilitate the sharing of information by a business about local citizens or businesses (Data Subjects) where the business reasonably considers it necessary or expedient:

- to allow the business concerned to comply with its reporting or disclosure obligations in any jurisdiction;
- to allow the business concerned to share information with a corporate affiliate to enable that affiliate to comply with its reporting or disclosure obligations in any jurisdiction;
- for the purposes of enabling the business concerned (or its affiliates) to make a fully informed decision about the risk of dealing with the Data Subject concerned or the risk of any transaction involving the Data Subject (including risks around fraud, AML and CFT).

G2G and G2B barriers could also be addressed by ensuring a **"gateway"** or exception to any Data Barrier to enable official sector authorities to share information with other authorities or with businesses, proactively or upon request, for similar purposes.

While such gateways could be limited to cross-border disclosures, to maximise the beneficial impacts on cross-border payments, such gateways should also cover domestic disclosures for the same purposes.

Any exceptions to the above gateways should be limited and strictly justified in terms of overriding public policy grounds.

Harmonization and standardization

Going forward, clarity, consistency, and the development of best practices around what kinds of data are subject to protections and higher compliance burdens would be positive. For example, inclusion of personal financial information in the definition of "sensitive" personal data creates increased restrictions around processing and cross-border transfer. It is excluded from that category in the GDPR but considered as such in India, Indonesia and Philippines.

Similarly, further progress should be made towards the harmonisation of international standards concerning AML/CFT information sharing. The IIF notes there is already a comprehensive set of recommendations of FATF in this area.[6] To the extent that Data Barriers arise from a failure to implement these recommendations fully and consistently, this is obviously of concern and one that the FSB could raise with the FATF.[7]

To increase payment message information standardisation and conformity will require action across multiple levels. Regulators and standard-setting bodies need to work in unison to drive greater clarity on the requirements to achieve standardisation and conformity of payment messages. Individual PSPs would then have clear obligations to ensure that customers are providing the required information and controls in place so that transactions can be completed without friction.

Alternatives to data localization

The IIF recommends that as a guiding principle, regulators and policymakers are encouraged to be clear on the regulatory objective for any data localization measure, demonstrate that the rules imposed are the least restrictive means of achieving those objectives, and remain open to new alternative solutions.

Means such as encryption and other privacy-enhancing technologies should be explored, wherever practicable, as alternatives to rules that balkanize the global data economy and prevent the full value of data from being realized, to the ultimate benefit of clients and end users.

For example, authorities concerned about unauthorised foreign access to data relating to local citizens may choose to make more use of encryption requirements instead of imposing data localization requirements. By requiring data to be encrypted, even if held offshore, with encryption keys held locally, authorities can ensure local control over access to data, while not preventing data being held where most convenient or efficient from the FI perspective.

Regulatory data access arrangements

Regulatory data access arrangements are a critical tool that can support the policy objectives of local authorities while also enabling cross-border data flows. Such arrangements can include contractual or public law measures to ensure authorities have access to the data they need from FIs to do their jobs, even if the data is held by third parties such as in offshore cloud facilities.

Intergovernmental agreements

Intergovernmental agreements can supplement efforts by industry and regulators to provide and secure data access or gateways, by ensuring Data Barriers are removed or addressed, for example by providing for access arrangements and gateways. Ideally, reference to data access arrangements and gateways would be written into this type of political agreement going forward.

Recent examples of international agreements with positive characteristics for the free flow of data include the Digital Economy Agreements and similar arrangements in place between

[6] See The Consolidated FATF Standards On Information Sharing (fatf-gafi.org) (November 2017).
[7] For more detail, see the section headed "Data frameworks and AML/CFT related issues" in Annex 2 to this letter.

Singapore and other jurisdictions including with Australia, with New Zealand and Chile, with the Philippines, and with the United Kingdom (in principle).[8] The IIF also notes the existence of the APEC Cross-border Privacy Rules System (CBPR System). The CBPR System applies to organisations (data controllers) that control the collection, holding, processing, or use of personal data and enables certified organizations across APEC economies to exchange personal data more seamlessly.[9]

MOUs

The IIF notes the European Supervisory Authorities (ESAs) approved on 10 January 2019 the content of a Multilateral Agreement on the means of exchange of information between the European Central Bank (ECB) and all competent authorities (CAs) responsible for supervising compliance of FIs with AML/CFT obligations under the fourth Anti-Money Laundering Directive (AMLD4). The Agreement is designed to create a clear framework for exchanging information between the ECB and CAs and potentially will enhance the effectiveness of their supervisory practices. In the IIF's view, this type of multilateral MOU (MMoU), which is well-known in the securities market sphere[10], would be beneficial on a global basis, or at least among FSB or FATF member jurisdictions.

Adequacy / equivalence assessments

While political agreements around the cross-border data elements of trade and commerce are clearly helpful, it is important that specific cross-border transfer regimes are subject to clear technical and legal assessment criteria (e.g., around adequacy and equivalence) rather than subject to political-level decision making. Timely adequacy assessments, such as those recently provided by the EU authorities, are also positive.

IT platforms

In terms of IT platforms, the trade reports exchange mechanism (TREM) operated by ESMA in the OTC derivatives trade reporting space may be a possible model for the exchange of information about cross-border payments, including a possible suspicious activity reports exchange mechanism (SAREM).[11]

4. Can approaches to data frameworks in one jurisdiction impact the provision or supervision of cross-border payments services in other jurisdictions? Are there particular issues that you would like to highlight?

Yes. Approaches to data frameworks in one jurisdiction can impact on cross-border payments that originate from or end in another jurisdiction, or in two third jurisdictions. This could be because the data frameworks apply to one or other end of the transaction, or because they apply to the FI concerned (e.g. if the FI is domiciled in that jurisdiction) which may be active in two other jurisdictions, including through restrictions on onward transfer of data. In a typical case, the inability to share personal identifying information or client information about a beneficiary or originator of a cross-border transaction may prevent the correct identification of the beneficiary or originator, or may prevent information known in another jurisdiction being used to make a risk assessment about that beneficiary or originator. Higher costs and operational complexity for all payments may result from the implementation of granular processes and controls to ensure payments data is fully compliant.

---

[8] See The Digital Economy Partnership Agreement (DEPA) (mti.gov.sg); UK agrees world's most comprehensive digital trade deal with Singapore - GOV.UK (www.gov.uk) (December); Australia-Singapore-Digital-Economy-Agreement (dfat.gov.au)

[9] See What is the Cross-Border Privacy Rules System | APEC

[10] See Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (MMoU) (iosco.org).

[11] See 2016-1521_mifir_transaction_reporting_technical_reporting_instructions.pdf (europa.eu), p. 4

5. **Are there particular payment corridors (especially related to emerging markets) that you wish to highlight to the FSB as facing specific challenges relating to data frameworks?**

In our recent report on Cloud Adoption and Regulation in Asia-Pacific Financial Services (Nov. 2021), jurisdictions mentioned as having very stringent data localization rules include Indonesia, South Korea, Thailand (in respect of health data), and China, where there are overlapping requirements emanating from a number of different levels of government and different authorities. India was cited by one FI as having data localization rules that were subject to changing (and increasingly stringent) interpretations over time. Our understanding is that India has imposed restrictions on the offshore storage and transfer of payments data, which limits domestic competition by requiring certain elements to be stored onshore while also creating challenges around scaling up domestic and cross-border services.

One particular frustration for regionally active FIs is those jurisdictions that provide for exceptions to data localization on paper, but where the process for activating those exceptions leads nowhere. In one example mentioned, in a regional economy, an FI decided to pull an application after 18 months of inconclusive discussion with the local authorities.

Annex 2

Further background to general remarks

Digital economic cooperation

Our recent IIF staff paper Strategic Framework for Digital Economic Cooperation (Oct. 2021) was sparked by industry leaders and public officials observing that we are fast approaching an inflection point and a "Digital Bretton Woods" may be needed to hammer out the new rules for a digital world. The Japanese G20 Presidency highlighted this challenge in 2019 with its "Data Free Flow With Trust" initiative, and we were pleased to see the notion of data free flow with trust at the heart of the recently adopted G7 Trade Ministers' Digital Trade Principles (Oct. 2021).

Against this background, we aim for our staff paper to provide a state of play outlining the problems and drawing attention to the potential harm that the global march towards a fragmented and isolated digital economic landscape could bring.

Unfortunately, the current global system and rulebook has been built for trade and flow of physical goods and is proving ill-equipped to deal with new challenges while maintaining free and open flows of data with trust. Instead, our current trajectory is moving toward an economic landscape that is increasingly national and protectionist in its tendency to apply old tools to new problems.

That trusted and permissioned flow, with economic and legal frameworks to ensure safety, security, and equal access opportunity, should be the goal of data policy.

Our Strategic Framework staff paper is soon to be followed by a further paper containing a recommended path forward.

The costs of data localization requirements

Previous IIF work, notably our report on Data Localization: Costs, Trade-offs, and Impacts Across the Economy (Dec. 2020), has examined how data localization measures can undermine many of the efficiencies and economic opportunities of the digital economy, imposing costs and risks across the economy, and impeding financial service efficiency, fraud prevention, and innovation.

It is laudable that governments are seeking greater privacy, security, and economic opportunity for their citizens in an economy increasingly dominated by hyper-scale technology companies; however, the data localization requirements currently spreading as a popular response, are constraining the flow and use of data while adding significant costs and trade-offs that are not generally understood or discussed.

Examples of the costs we identify, many of which are directly relevant to cross-border payments, include:

- Derailed fast payments, low-cost remittances, and other services individuals, households, and small business need to function in the digital economy.
- Weakened fraud prevention, cyber security defense, and potential new AML solutions.
- Blocked innovation and competition through curtailed access to the public cloud, a key enabler to the development of fintech and other innovative start-ups by providing low entry costs, scalable platforms, and embedded services.

- Reduced access to the best and newest cloud-based software, technology, and future cloud first technologies such as quantum computing.

- Undermined cost effectiveness of cloud-based computing.

- Reduced connections to digital trade, negative impact on economic growth and development, and constrained ease of doing business.

- Weakened resilience of the financial system. The ability to have seamless failover redundancy systems and storage outside geographical borders could be essential in the case of a natural disaster, war, or other catastrophic event.

- Added costs of redundant local data infrastructure that was estimated at between $350 million to $800 million (Lafferty).

Cloud computing, data localization, and payments

In our recent report Cloud Adoption and Regulation in Asia-Pacific Financial Services (Nov. 2021), we highlighted the nexus between cloud computing, payments and data localization. Payments, including remittances, are a particularly relevant source of use cases for cloud gaining in prominence in Asia-Pacific. Remittance flows present a promising use case for cloud technologies to reduce costs and promote interoperability across different payment rails.[12] Many "paytechs," including names active in Asia-Pacific such as Wise, Revolut and NIUM, are of course entirely or largely cloud-native.

The report's findings were based on written or oral interviews with senior representatives of 15 official sector agencies (central banks, monetary authorities, bank supervisors and securities regulators) across 10 Asia-Pacific economies. The IIF also held focus groups and bilateral discussions with FI members based or active in the region and engaging with cloud adoption issues. Those engagements were conducted in September – November 2021.

FIs we asked about regulatory pain points in framing this report tended to revert to the topic of data localization. The FIs we engaged with said that data localization requirements, particularly the second and third types, can have several important negative effects:

- limiting the economies of scale that would otherwise be reaped from cloud solutions;

- increasing cyber risk by increasing the attack surface for cyber-attacks;

- reducing or eliminating the scope for data aggregation, and therefore limiting the ability to accurately model global risk, and limiting the effectiveness of anti-fraud or AML systems.

The authorities we interviewed expressed a variety of attitudes to whether data relating to FIs or their clients should be held locally (either in local copy or by prohibiting export), but all jurisdictions insist on ready regulatory access to data held in the cloud as being key.

> *The key consideration remains that we must have unfettered access to bank data required for discharging its regulatory function. The same principle applies to cloud outsourcing, which is a type of technology outsourcing. We believe our focus on supervisory access does not, and would not, cause barriers for technology adoption, including cloud adoption.* – ***Monetary authority***

[12] Digital Monetary Institute (DMI) and AWS Institute (2020), Enabling financial inclusion in APAC through the Cloud (25 November), p. 19. In writing this report, the authors surveyed and consulted 18 policy-makers, regulators and officials from central banks, supervisory authorities and international organizations. Of these institutions, 16 were from East, South and Southeast Asia.

Jurisdictions with data localization rules cited a wide variety of regulatory objectives, for example protecting national security, protecting individual privacy, securing ready access to data for law enforcement or for supervision or resolution authorities, increasing economic growth or employment or ensuring self-reliance, preventing foreign surveillance, enforcing data protection laws, and mitigating geopolitical risk from spilling-over to the domestic system.

Many jurisdictions make an exception from data localization rules for foreign-headquartered banks; however, as mentioned above, the experience of FIs can be that such exceptions can be difficult and time-consuming to try to utilize, without guarantee of success.

Using encryption as an alternative to data localization

Interestingly, one jurisdiction mentioned seeking to ensure that foreign regulators, law enforcement or security agencies cannot access data without permission by requiring that data is encrypted at the cloud service provider, and that encryption keys remain local, even if data is held remotely.

This appears to the IIF to be a pragmatic and desirable approach that delivers key regulatory objectives (i.e., preventing unauthorized foreign access, and having a means of data access in the jurisdiction) without requiring that the actual data be held locally. Nevertheless, if there is no local custodian of encryption keys, it may heighten cybersecurity risk to require FIs to be custodian of their own keys.

Recommendations on data localization

In this report, the IIF recommends that as a guiding principle, regulators and policymakers are encouraged to be clear on the regulatory objective, demonstrate that the rules imposed are the least restrictive means of achieving those objectives, and remain open to new alternative solutions.

Means such as encryption and other privacy-enhancing technologies should be explored, wherever practicable, as alternatives to rules that balkanize the global data economy and prevent the full value of data from being realized, to the ultimate benefit of clients and end users.

Data frameworks and AML/CFT related issues

This global problem is not only encountered where FI seek to share intelligence with foreign law enforcement or other institutions, but can manifest itself within a banking group, where some jurisdictions impose limitations on sharing data on a group-wide basis.[13] New technology for risk management and compliance in this area will also struggle to reach its full potential if the correct, good quality data is unavailable to facilitate machine learning and other activities which can help to achieve better outcomes. Possible mitigants such as "federated learning," even if technically feasible and well-understood, may only go part of the way to addressing these issues.[14]

When considering domestic and cross-border data exchange, it is also important to emphasize that data protection and data privacy 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 to sharing

[13] For further analysis, the IIF previously 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 contained information concerning 92 countries across Europe, North America, Asia, Africa, Latin America and the Middle East. The report can be found here: https://www.iif.com/publication/regulatory-report/iif-financial-crime-information-sharing-report

[14] See FCA, 2019 Global AML and Financial Crime TechSprint

information on illicit financial activity where necessary to limit its furtherance. This topic has been recognized by the FATF in changes to FATF Recommendation 2 (as noted below) when considering the compatibility of AML/CFT and data protection rules and should be addressed more widely at the national and regional levels.

In tackling these issues, the IIF supports the Roadmap's efforts to deal with constraints on cross-border data sharing. Critically, the adaptation of data sharing rules and supervisory and oversight standards to facilitate cross-border exchange of data should be addressed holistically on an international basis.

Consideration of the following issues would further the goals of the official sector on improving confidence between FI and between jurisdictions, thus facilitating cross-border data flows and fostering improved digital identity frameworks and shared customer due diligence infrastructures – all of which would benefit an enhanced cross-border payments architecture:

1. Harmonized Implementation of International Standards Concerning AML/CFT Information Sharing

Effective implementation of the current FATF Recommendations 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 authorities 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 countries with an eye toward ensuring practical and tangible outcomes which improve the environment for exchanging intelligence.[15]

Setting up an international forum for cooperation between data protection authorities and AML/CFT authorities should also be considered in order to develop better lines of communication across jurisdictions on these issues in order to facilitate greater consistency in approaches and further cross-border information exchange.[16]

We encourage member jurisdictions of the Basel Committee on Banking Supervision (**BCBS**) and beyond to consistently implement guidance on sound management of risks related to money laundering and financing of terrorism which enables greater interaction, cooperation, and information exchange between AML/CFT and prudential supervisory authorities.[17] 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.

2. Further Updates to International Standards Concerning AML/CFT Information Sharing

We have encouraged FATF to continue to work to improve the effectiveness of its member states' information sharing regimes. Specifically, as the FATF Recommendations offer a comprehensive and coherent framework of measures which countries should implement in order to combat money laundering and terrorist financing, the IIF believes that the

[15] For further information on these issues, please see IIF Staff Paper on Financial Crime Intelligence Sharing (Oct, 2020).

[16] This concept is discussed further on pages 19 and 20 of the White Paper: IIF/Deloitte, *The effectiveness of financial crime risk management reform and next steps on a global basis,* November 2021. *https://www.iif.com/Portals/0/Files/content/Regulatory/11_15_2021_fin_crime_deloitte_iif.pdf*

[17] 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

Recommendations would benefit from incorporation of the following principles in order to enable more effective information sharing consistently applied across jurisdictions:

- Jurisdictions should ensure that secrecy and privacy laws, and tipping-off or similar provisions, do not inhibit the exchange of relevant information, including Suspicious Activity Reports (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. Countries should ensure that adequate legal protections for banks that share information in good faith are in place to facilitate the sharing of such information.

- Jurisdictions should ensure, 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.

- Jurisdictions should ensure, where an entity is required to report a suspicion which relates to activity across a number of group enterprises or jurisdictions, that the applicable laws facilitate the filing of identical reports in each relevant jurisdiction.

3. National and Multilateral Public/Private Sector Information Sharing Development

In addition to critical enhancements to – or implementation of – international standards in this area, it is also important to facilitate information sharing between the public and private sectors through jurisdiction- and region-led initiatives. At the center of an intelligence-led financial crime mitigation model is the public/private partnership (**PPP**), a collaboration between FIs, law enforcement and the regulatory community. Jurisdictions and regional bodies should continue to actively support the creation of PPPs as a means to advance information sharing goals. PPPs are an important first step in the ability to deliver operational benefits and efficiency gains, and they can 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. Where there is statutory underpinning for PPP data sharing, this can also expedite overcoming some of the impediments outlined herein. [18]

FSB's prior work on data barriers

The IIF would recall that the FSB has undertaken detailed work on data barriers in the context of OTC derivatives data sharing that may be quite informative to the present work.[19]

The data barriers concerned in that work related to barriers that would prevent reporting entities reporting full trade data to trade repositories, and also that would prevent authorities from accessing trade data held in trade repositories.

[18] For further information on public-private partnerships, please see: IIF/Deloitte, The Global Framework for Fighting Financial Crime: Enhancing Effectiveness and Improving Outcomes, October 2019: https://www.iif.com/Publications/ID/3606/The-Global-Framework-for-Fighting-Financial-Crime-Enhancing-Effectiveness-Improving-Out-comes

[19] See FSB (2018), Trade reporting legal barriers: Follow-up of 2015 peer review recommendations and FSB (2015), Thematic Review on OTC Derivatives Trade Reporting: Peer Review Report.

In the cross-border payments space, there are similarly three distinct levels of barrier that may be relevant and should be considered separately:

- Data flows between different private sector entities, within or without corporate groups;
- Data flows between private sector entities and authorities;
- Data flows between authorities.

The barriers identified were classified as arising from official requirements relating to data protection, client confidentiality (such as banker secrecy), blocking statutes (such as state secrecy legislation) and other data barriers. A similar taxonomy of data frameworks could be useful to clarify where the key issues lie.

The FSB found that barriers to data sharing, particularly those arising from data protection and client confidentiality requirements, could be addressed with client consent, which may be able to be given on a standing basis. In its comment letter dated 13 July 2018, the International Swaps and Derivatives Association had argued that due to a number of reasons, including operational burden and challenges, consent requirements form a barrier in their own right and should be removed for reporting of trade data pursuant to both domestic and foreign trade reporting.[20] Taking into consideration the concerns expressed, the FSB was of the view that these concerns were outside the scope of the follow-up work and therefore as long as reporting pursuant to such requirements is permissible with counterparty Consent, and Standing Consent is available, this was considered sufficient to address the relevant barrier.

In the cross-border payments context, we would urge reconsideration of this issue. A requirement for client consent, where the client has no incentive to cooperate (for example where the FI is unable to impose the requirement for consent as a term of doing business), may in practice represent a significant barrier.

Another issue considered in that FSB work was the significance of the requirement that the consent of a local regulatory authority be obtained before data may be shared across border. We would agree with the FSB's characterization of that as a barrier, at least where there is no guidance to the effect that consent will be forthcoming.[21]

Lastly, that work highlighted the key important of inter-agency Memoranda of Understanding (**MOUs**) and other operational arrangements for data sharing across borders between authorities, and engaged in a mapping exercise that shows a certain degree of MOUs in place among the key FSB OTC derivatives markets. It could be useful for the FSB to build on or update this work with a specific focus on payments related information, given the authorities involved will in many cases be quite different.

[20] FSB (2018), *op. cit.,* p. 5
[21] FSB (2018), *op. cit.,* p. 6.