Recommendations for Regulating and Supervising Bank and Non-bank Payment Service Providers Offering Cross-border Payment Services: Consultation report

Response to Consultation

UK Finance

Introduction

1. **Do the definitions contained in the report provide sufficient clarity and establish the common understanding necessary to facilitate the practical implementation of recommendations proposed in this report?**

   Our members welcome the fact that the global authorities and standard setting bodies have sought to collaborate, across regional regulators, to design and agree common standardised definitions.

   Generally, the FSB has captured the role of banks and NBPSP accurately; however, below we set out further considerations and share examples from international jurisdictions:

   Activity-based versus Entity-based regulation: We note that the definitions distinguish between activity-based regulation and entity-based regulation and that the FSB has acknowledged in the latter definition that "Competent authorities may also adopt a hybrid approach that combines elements of both activity- and entity-based regulation depending on the nature of each jurisdiction's regulatory structure".

   Increasingly we are seeing the authorities in the UK and elsewhere converging around the principle of "same activity, same risk, and same regulation". We are supportive of that as a broad concept, but the approach inevitably requires fine tuning when it comes to the detail of the specific issue, circumstances and application to ensure a proportional approach and to avoid unintended consequences.

2. **What adjustments are required to the draft definitions to improve clarity?**

   Definition of payments: The FSB has stated that the proposed definition of payments is intended to "cover all types of electronic funds transfers and instruments (e.g. cheques, credit transfers, direct debits, card payments, e-money)". We think it would make sense to add instant/fast payments to the list as this payment type is gaining increasing focus in the market and tends to be distinguished from 'standard' credit transfers. Historically, paper-based instruments such as cheques are sometimes treated differently from electronic

payment types from a regulatory perspective. Any differentiation in treatment of any instrument, including emerging developments around digital currencies, needs to be made clear at the outset. We would recommend an agile approach to reviewing the definition as the ecosystem continues to evolve.

Definition of payment system: The FSB has defined the term “Payment System” as a “set of instruments, procedures and rules for the transfer of funds between or among participants” which is taken from the ‘Principles for FMIs”. There is a risk that such a definition may not sufficiently address scenarios where there is a clear delineation between scheme and infrastructure, which in turn results in different roles and responsibilities.

For example, in the context of SEPA, there is a difference between: (1) the SEPA

scheme rules managed by the European Payments Council in its role as SEPA

scheme manager; and (2) SEPA-compliant Clearing and Settlement Mechanisms

(such as EBA Clearing’s STEP2, which has its own rules that align with those set by

the scheme). Again, we would recommend that the definition is reviewed as the

ecosystem evolves to align with the "same activity, same risk, same rule" principle.

We suggest that the Wolfsberg Group, association of 12 global banks which aims to develop frameworks and guidance for the management of financial crime risks, provides a good example in seeking the inclusion of the Payment Market Infrastructures as well as FMIs in the definitions as both are critical to solving for a number of the issues identified.

3. What other terms should be defined in this section?

Market practices: in reviewing the definitions put forward in the report, the FSB may wish to consider the implications of market practices and conventions. For example, we note that the focus of the FSB’s Recommendations is on retail payments. Traditionally, a distinction has tended to be made between Large Value Payment Systems (high value, low volume) and retail payment systems, which the FSB describes here as “high volume, low value transfers”. We agree that it makes sense to differentiate between wholesale and retail payments however we question whether today it still makes sense to refer to value as part of the definition. For instance, in the UK, the Faster Payments System would be classified as a retail payment system, yet the scheme rules allow for a maximum transaction limit of £1 million.

It is important that the FSB continues to have an approach to harmonising international requirements, as set out above, that ensures that the ecosystem is regulated end to end. As the payments ecosystem continues to evolve, regulators will need to adopt an agile approach to the definitions ensuring that they are reviewed on a regular basis and incorporate emerging business models across the payments ecosystem. For example, it may be necessary to extend the scope to include support services in the future. Requirements will need to remain sufficiently detailed and clear to ensuring a level playing field where NBPSPs are subjected to similar regulation as banks, and key to this is fairness and resilience, and critically, protection of customers.

4. **Does the explanation regarding the scope of the report provide sufficient clarity to promote the intended understanding of the recommendations?**

See our comments above.

Section 1: The role of banks and non-banks in cross-border payments

5. **Do the descriptions of the roles of banks and non-banks in providing cross border payment services adequately reflect current practices?**

The multiplicity of banks and NBPSPs operating in the payments landscape supports the diversity of business models, innovation, competition and, ultimately, choice for payment service users.

The FSB report provides a good overview of how the roles of bank and NBPSPs and their interrelationships have evolved and, here, we set out further considerations and provide examples.

NBPSP access to payment systems and accounts with central banks: The report makes reference to restrictions applying in "most jurisdictions" to NBPSPs' ability to access systemically important payment systems and maintain settlement accounts with central banks.

We note that these are areas of focus in the UK and European Union.

- For example, the Bank of England already permits NBPSPs to access RTGS and earlier this year issued a Discussion Paper on "Reviewing access to RTGS accounts".

- The European authorities have recently approved changes that are being introduced through the new Instant Payments Regulation, which are intended to improve NBPSPs' access to payment systems and give NBPSPs the option of safeguarding users' funds in an account held at a central bank where the latter (at its discretion) provides such a possibility. In July 2024, the European Central Bank published its Policy1 in this regard. The policy allows NBPSPs established within the EEA access to all Euro area central bank-operated payment systems (not only TARGET) provided that all necessary risk-mitigation requirements are in place. However, a decision has been taken that Eurosystem central banks shall not offer safeguarding accounts to NBPSPs on the basis that this is not a core function for central banks and brings with it a range of risks which are detailed in the policy document.

1 https://www.ecb.europa.eu/paym/target/target-professional-use-documents-links/tips/shared/pdf/Eurosys_pol_on_access_to_central_bank_operated_payment_systems_by_NBPSPs.pdf

Direct versus indirect payment system access: An increasing number of jurisdictions are exploring forms of direct access for non-banks, with the US being the only G7 outlier. A recent CPMI survey also indicated that "jurisdictions that have expanded their access policy, particularly to NBPSPs, did not report major negative impact to the structure or operation of their payment systems. However, next to a growth in transaction volumes, several payment

systems reported increased need for help desk support and a rise in operational incidents (including cyber-attacks) as an impact of a change in the composition of participants accessing the payment

system." This example showcases that some of the perceived risks that NBPSPs may pose to payment systems fail to materialise if the right mitigating measures and supervisory criteria are introduced.

Inevitably direct participation brings with it certain expectations and responsibilities, which are necessary to mitigate risks of failure to maintain mutual trust and financial stability. For instance, the first non-bank PSP given access to CHAPS in the UK, entered administration a year later, which emphasises the importance of ensuring that appropriate controls and preventative measures are in place to protect the integrity of the payment system and to avoid placing an increased or disproportionate risk on other participants

There should continue to be recognition that for some bank and NBPSPs direct participation may not be the ideal solution and they may prefer to participate indirectly. Accordingly, support for such arrangements should continue. We note the work done in the UK by the Payment Systems Regulator and at industry level to promote greater transparency on the part of sponsor banks to make it easier for indirect participants to compare service offerings. This is indicative of the positive role that competent authorities and industry associations can jointly play in facilitating broader awareness and understanding of the different options available.

Supervision for NBPSPs: Some of our members believe that as part of license applications and supervision, non-banks should consistently be assessed as part of BAU supervision. However, as non-banks still have to rely on banks for a large part of their operations, supervisors may be tempted to rely on the due diligence banks perform on their non-bank partners. While the due diligence of banks is always carries out to a high level, they may not have the full cross-market purview of a supervisor. This can lead to a knee-jerk reaction if something goes wrong and can result in an unnecessary clampdown, prohibiting or limiting certain business models or activities. In addition, in some countries providing cross-border payments or remittances are restricted for non-banks.

The requirements of supervisors sometimes mean that for some NBPSPs there is a risk of being de-banked across jurisdictions. Banks may be required to off-board NBPSPs or withdraw from servicing NBPSPs altogether as they seek to meet their own compliance obligations. Some of our members view this as an inherent barrier to competition within the payments market. It also means that the customers of the NBPSP - as well as non-customer recipients - can lose access to a service they relied on from one day to the next, while the NBPSP looks for a different partner and needs to negotiate a new deal in a weaker position. Re-opening that service may come at an increased cost.

In addition to the risks surrounding non-bank access to payment accounts, the report rightly notes that non-banks also rely on banks to maintain segregated accounts for client funds with commercial banks or 'safeguarding' of customer funds. As non-banks grow in size, some members feel that there is increasingly less to no choice between providers with which they can safeguard their customer funds, especially when certain jurisdictions mandate having at least two safeguarding accounts. This leads to non-banks becoming increasingly

clustered around a small number of banks that are large enough and have the risk appetite to hold billions in segregated customer funds. Some of our members believe that one approach would be enabling safeguarding at central banks as an additional option for non-banks, they would gain access to a broader range of diversification possibilities for safeguarding their customer funds. This is already possible in certain countries and helps reduce concentration risks, lower the risk profile of safeguarded funds, mitigate third party de-banking risks and increase consumer trust in safeguarded funds.

Diversity of payments business models: In the context of cross border payments, it is necessary to capture all firm types as there are long standing alternatives to banks, such as money transmission bureaus and Fintechs whose models eventually rely on traditional banking systems to move money. Managing the risk of these models is important.

A future view is also needed as big tech moves into the cross-border payment space and the consequences considered from a regulatory point of view. Consideration needs to be given as to how this model can be actively regulated to protect customers.

In addition, ACH to ACH models are emerging as ISO 20022 standards are adopted, and consideration should be given as to how to regulate and monitor these models too. The topic of regional models is interesting especially after failed attempts in the Nordic region (due to lack of agreement on the "Central Bank" for 5/6 currencies), but the successful implementation of BUNA in the Middle East is worth noting. Other initiatives, such as BIS Agorá should also be considered.

Payment mechanisms such as CBDC and digital currency are in active development globally on a regional and country basis, but it is unclear how they would work in a cross-border environment. It is important to consider whether the central banks need to have agreements in place with each other to make global cross border payments more straight forward in the future whilst maintaining security and integrity.

Section 2: Cross Border Payment Frictions and Risks

6. What additional risks or frictions, within the scope of this report, are created by potential inconsistencies in the legal, regulatory and supervisory frameworks applicable to banks and non-banks in their provision of cross-border payment services?

Our members broadly agree with the risks and frictions caused by inconsistencies in the legal, regulatory and supervisory frameworks, and identified by the FSB. Here, we set out additional considerations:

Fraud: As the speed and ease of making a payment increases, this can make fraud and other economic crime easier to perpetrate. We encourage the FSB to consider ways in which regulators can collaborate internationally to establish ways for criminally acquired funds to be returned, confiscated or otherwise repatriated to appropriate authorities.

Different applications of global financial crime and fraud standards can create friction and credit risk in provision of cross border payments. An example would be recent issues some members have seen in applying a hold for cover parameters to inbound cross border

payments, whereby straight-through-processing of inbound payments (rather than waiting for cover funds) has on a number of occasions seen some members out of pocket as the beneficiary bank, on the basis of differing application of localised financial crime policies through intermediary banks. Inconsistent application of AML/CFT regulation can impact on STP and cross-border settlement.

It is worth highlighting that the root causes of fraud can't be tackled by the financial services industry alone. It is crucial that the whole fraud chain is brought in to ensure higher levels of consumer protection and lower levels of fraud. For example, analysis in the UK shows that 70% of APP scams2 started on an online platform, defined as emails, social media, websites (including auction sites), and apps (including dating apps). Often these are paid-for advertisements, meaning that social media companies are profiting from fraudulent ads while the finance sector bears the brunt of the cost. In many jurisdictions, there are live conversations around the inclusion of online platforms, including social media platforms, into any fraud mitigation response. Collectively, this would help tackle fraud at source instead of focusing solely on financial institutions as the last stage in the fraud value chain. We believe that this is a crucial and global step and would encourage the FSB to investigate a global coordinated response.

In addition, the FSB highlights that NBPSPs are more likely to engage in "occasional

transactions" and while that may be true for some companies, it's worth highlighting that many NBPSPs tend to be younger companies, starting from the first fintech wave in 2010-2015. This means that they often don't have the same long-established client relationships to fall back on as banks do. While transaction monitoring is often paired with machine learning and AI to combat financial crime from taking place on their platforms, the lack of history can sometimes pose risks which could be addressed by stronger information sharing between the financial services industry. Financial crime remains a joint fight.

Consumer protection: The FSB report rightly references consumer protection as one of the risks. In developing measures designed to support or protect consumers, regulators should keep in mind that payments (whether domestic or cross-border) need to suit a range of needs and different types of users. Therefore, it should be borne in mind that some measures may be inappropriate or require re-configuration for the corporate space.

Domestic and international payment chains: In many jurisdictions, there is no mechanism to recognise that a domestic payment is part of a chain of a cross-border payment. Where local payment rails are used to send international transactions, payment infrastructure limitations can obstruct the inclusion of additional payer or payee data. Even if the additional information is included in the payment message, the information would not necessarily be captured by the recipient's financial institution because they would automatically classify it as domestic. We believe that this is an issue stemming from current payment infrastructure limitations rather than from specific payment business models, but it is an area where changes to domestic payment infrastructure could make a real difference to innovation in the processing of cross-border payments. This also has an impact on financial institutions' ability to apply the appropriate sanctions screening.

Scope of application of any requirements: There needs to be clarity on the scope and application of any associated legislative framework and, where appropriate, there should be

an ability to apply a “corporate opt-out” – as is the case with the EU’s Payment Services Directive.

ML/TF: The FSB paper usefully points out that: “…while a jurisdiction’s regulatory requirements for CDD and suspicious activity monitoring generally will apply to both banks and NBPSPs, the supervisory approaches for enforcing such compliance often vary, especially if the AML/CFT and prudential supervisors are different or if the jurisdiction does not require licensing of all non-banks PSPs. Since most NBPSPs currently access national payments systems through banking relationships, in those circumstances where the PSPs do not establish customer relationships that facilitate the conduct of effective CDD, the bank’s exposure to ML/TF risk may be increased. Supervisors in turn may view those increased risks as not sufficiently mitigated by controls established under the bank’s AML/CFT compliance programs.” There needs to be a level playing field and it is not proportionate to expect banks to take responsibility for conducting CDD on their clients’ clients.

Capital controls: there are inconsistencies in the application of “beneficiary verification”, i.e. imposing verification on the end-beneficiary. This is generally overly burdensome. PSPs do not have relationships with the beneficiary. They are required to contact the recipient with insufficient contact data and go through the verification process before the payment can proceed in where they are not known to the recipient. This adds to the time and friction to the payment process.

Impact of emerging business models: Application of FATF Recommendation 16 is not universal, and it can be difficult for banks to police as payments landscapes evolve rapidly. We encourage the FSB to set out how national regulators can more consistently apply these requirements in line with the ‘same activities, same risk, same regulation’ principle.

It may be useful to consider adding further examples to the report. For example, Automated Clearing House (ACH) transfers where there is a lack of infrastructure to support compliance with requirements and leads to truncation of data could lead to inconsistent application of the rules, impeding effective monitoring and compliance with the Funds Transfer (Information on the Payer) Regulations.

While the FSB refers to FATF’s R.16, it is worth noting that this was originally drafted with a correspondent banking model in mind, assuming that international transactions include routing of transaction messages via a centralised messaging system (such as Swift). In contrast, some companies facilitate cross-border payments by making two domestic transfers rather than going through the correspondent banking network.

Lack of harmonisation in licensing frameworks is detrimental for firms looking to operate cross-border. While certain countries have replicated frameworks that broadly mirror the UK/EU (with payment institution and e-money licenses), other jurisdictions still take a bank vs non-bank approach without recognising varying permissions in the non-bank framework. There is no “sliding scale”. It is worth noting that introducing licensing regimes such as the UK and EU has also brought these non-banks into the regulatory framework of other legislation, such as rules around operational resilience. This is ultimately beneficial for the ecosystem as a whole.

Section 3: Principles for developing recommendations

7. Do the identified principles provide sufficient support and appropriately frame boundaries for the recommendations in the report?

The principles usefully highlight the importance of resilience, efficiency, proportionality, cooperation, coordination, and responsiveness to change.

While the principles are sensible, their interpretation in practice will require debate and widespread global understanding. For example, addressing issues such as how will proportionality play out in practice? Is there a risk of a lowest common denominator? Conversely will some parties use the cross-border principles to insist on practices required in their own jurisdiction to be used in other jurisdictions?

Thus, we see that though a more harmonised cross-border regulatory regime is desirable, it will be important that regulatory and supervisory bodies ensure on-going alignment is maintained. Any harmonisation must be proportionate to the perceived risks and must avoid gold plating and regulatory arbitrage. Alignment of regulatory regimes must be an enabler of cross-border payments, not introduce undue frictions. An example of potential overreach would be FATF's recent consultation on FATF Recommendation 16 which considered a potential requirement for receiving PSPs to verify payee details in the payment message against KYC details on file – a potentially material step change that could have a significant impact on STP for cross-border payments.

The complexity and challenges of these cross-border principles is only illustrated by the fact that we appreciate that there will from time to time be genuine reasons why particular states would have a need for local rules.

Section 4: Recommendations for improving alignment of PSP regulatory and supervisory regimes

8. Are the recommendations sufficiently granular, actionable, and flexible to mitigate and reduce frictions while accommodating differences in national legal and regulatory frameworks and supporting the application of proportionality?

We note that the six policy recommendations in the consultation report are directed at competent authorities who may be better placed to determine whether they are sufficiently granular, actionable, and flexible. They are helpful, however, in setting out areas competent authorities should consider from a cross-border payments perspective and providing a foundation to support greater consistency.

We also note that bridging the gap between recommendations and detail of national, legal and regulatory frameworks is going to be challenging unless there are agreements between specific regulators in different countries.

We set out our views of the Recommendations:

Recommendation 1

We welcome the fact that the stated intention under Recommendation 1 is to achieve “a level-playing between bank and NBPSPs that reflects the principle of “same activity, same risk, same rule”, while taking into account the differences in risk profiles” and agree that this “requires a comprehensive and sophisticated understanding of PSPs’ activities and their risks as well as on potential mitigants to ensure the safety and efficiency of cross-border payment services”. Such mitigants should also be proportionate and allocate responsibilities and expectations fairly between the parties.

We would appreciate further clarity on, for example, do Competent Authorities look

only at PSPs registered in their jurisdiction and are they expected to allow others to

operate in their territory? Also if there is a passporting regime in place.

Recommendation 2

The recommendation seeks to ensure consistency, but it is important to acknowledge that in some instances a one-size-fits-all approach may not be appropriate to accommodate the variety of business models in the market. The more informed competent authorities are - especially in the context of new, emerging products and services - the better, so engagement with industry will also be key to avoid misunderstandings and unintended consequences.

Recommendation 3

This recommendation could be more granular and actionable. It states that “consumer protections should include ensuring transparency with respect to payment service delivery and pricing of services”. It could further refer to the G20 Cross-border payments roadmap goals, particularly on transparency of fees. Some members propose that this should include FX margins, which - to the FSB’s own admission - make up a large proportion of the cost of a cross-border payment.

Our members would encourage the FSB to ensure that consumer protection requirements apply to both banks and NBPSPs. In addition, the FSB should further clarify targets and metrics regarding transparency on transfer pricing. This is currently falling by the wayside, with many jurisdictions focusing on speed disclosures or singling out upfront fees, while disregarding FX

margins.

We also note that consumer protection shouldn’t be a competent authority’s’ sole objective, giving the example of the FCA in the UK, whose operational objectives are to:

- protect consumers from bad conduct,
- protect the integrity of the UK financial system,
- promote effective competition in the interests of consumers.

Since 2023, the FCA has had a secondary objective to facilitate the international competitiveness and growth of the UK economy in the medium to long term (subject to alignment with international standards).

It is also important to consider implementation detail. For examples, how will

consumers action their protections? In which jurisdiction will they have rights? Can

they always go through their own PSP? How will that PSP secure resolution a

miscreant in another jurisdiction?

To make these recommendations effective the FSB will need to secure agreement

between many national authorities on how consumers can action their cross-border

rights.

Recommendation 4

We support the idea that competent authorities should communicate clearly their expectations directly to the market and relevant parties (be they bank or NBPSPs or direct and indirect payment system participants). We also agree that the provision of “dedicated assistance” to PSPs (such as workshops) by competent authorities is welcome.

- From a UK perspective we have seen the benefits arising from publication of the Financial Conduct Authority’s Payment Services Approach Document as a way of providing guidance.

- At EU level, recent workshops and subsequent publication of the European Commission’s Clarification of requirements of the Instant Payments Regulation provides another example of an approach to promote consistent interpretation of text.

To further alignment and best practice, outputs from focus group discussions and

supervisory practises must be shared, rather than encouraged, with other

jurisdictions if consistency is to be a stated aim, although we expect this would be

difficult achieve. There will be a requirement for a body to orchestrate and best

practice is implemented. There is a potential gap in rules and responsibilities which

may be filled by FSB issuing market guidance.

Recommendation 5

We are strongly supportive of Recommendation 5 as a way to promote a level playing field but also to provide a stronger basis for successful partnerships between banks and NBPSPs, for example in the context of payment facilitators for payments into wallets.

We note that the FSB states that Recommendation 5 “focuses on domestic licensing” and is asking “How and to what extent would licensing recognition regimes between jurisdictions support the goal of strengthening consistency in the regulation and supervision of banks and non-banks in their provision of cross-border payment services?” The more that licensing regimes are aligned, and firms are held to similar standards regardless of jurisdiction, the greater the level of consistency that can be achieved. This still runs the risk of competent authorities interpreting requirements in very different ways. This is where having global-level agreement on minimum requirements could prove beneficial

The huge success of the EU’s licensing regime, which enables passporting of services across all countries in the EU cannot be overstated. It’s evident by the sheer number of payment and e-money institutions offering their services across the EU’s Single Market. This significantly benefits citizens from markets without major payments players of their own, as they can still reap the benefits of the services those PSPs offer when they might not have considered entering that market if passporting hadn’t been available.

The EU’s system of mutual recognition of licensing both within the EU and some

third countries would be similarly beneficial if extended to other pairings of

jurisdictions. For example, in a hypothetical scenario, a recognition agreement

between UK and South Africa (SA) would give leeway for payments coming from SA

and PSPs sending from SA that could be accepted into UK without such detailed

checks.

Equivalent licencing regimes would support cross border payments, however, regulators would need to consider the liability of firms in one jurisdiction to firms in another on items such as consumer protection or errors made in payment processing.

It is not simply initial (and ongoing) alignment between payment licensing but also

Wider societal change and best practice that may require ongoing alignment. There

is also the question of how and to what extent would licensing recognition regimes

between jurisdictions support the goal of strengthening consistency in the regulation

and supervision of banks and non-banks in their provision of cross-border payment

services? What risks need to be considered?

Recommendation 6

We strongly agree with the statement in the paper underlying Recommendation 6 that says that “cooperative arrangements among regulators should be transparent to PSPs, other financial institutions and third parties so they can understand the regulatory environment and meet their customers’ expectations and regulatory obligations, as well as consumers”.

Relevant authorities should ensure that there is sufficient information sharing across jurisdictions, so 'host' states can increasingly rely on 'home' state requirements without introducing additional burdens that become barriers to expansion for PSPs operating globally or across borders. This includes data localisation requirements which are often burdensome, decrease operational resilience & data protection and add to financial pressures as they often lead to significant additional headcount. In addition, AML/CTF requirements should follow global rules and standards.

Policymakers will need to consider how financial institutions can share more information with competent authorities and with other industry participants within the relevant privacy frameworks. Today, these frameworks hamper the introduction of a strategy that would combat financial crime and fraud effectively. The fraud chain often starts online and today, online platforms and the financial services industry are unable to work together to tackle the root causes of these types of financial crime.

From a priority and effectiveness perspective, our members suggest that the focus for should be on facilitating the implementation of already agreed global standards and targets, such as those set out in the G20 Roadmap for enhancing cross-border payments.

As the proportion and value of payments sent via non-banks increases, in order to protect customers and ensure the stability of the system, comprehensive international standards for the regulation and oversight and supervision of banks and NBPSP will become essential. This will only be meaningful if there are agreed minimum standards. These should, among other things, liability and further clarity to meet requirements. Critically, the implementation of these initiatives and recommendations is key.

9. **To what extent would the recommendations improve the quality and consistency of regulation and supervision of non-bank payment service providers (PSPs) active in cross-border payments services?**

   See our comment above

10. **For the purpose of identifying material areas to be addressed from a priority and effectiveness perspective, should the report categorise the identified frictions created by inconsistencies in the legal, regulatory and supervisory frameworks applicable to banks and non-banks in their provision of cross-border payments services in terms of focus or order in which they should be addressed?**

    See our comments above, and to reiterate: From a priority and effectiveness perspective, our members suggest that the focus for should be on facilitating the implementation of already agreed global standards and targets, such as those set out in the G20 Roadmap for enhancing cross-border payments.

11. **Recommendation 5 focuses on domestic licensing. How and to what extent would licensing recognition regimes between jurisdictions support the goal of strengthening consistency in the regulation and supervision of banks and non-banks in their provision of cross-border payment services? What risks need to be considered?**

-

12. **There are no comprehensive international standards for the regulation, supervision and oversight of non-bank PSPs and the cross-border payment services that they offer. Is there a need for such international standards?**

    As the proportion and value of payments sent via non-banks increases, in order to protect customers and ensure the stability of the system, comprehensive international standards for the regulation and oversight and supervision of banks and NBPSP will become essential. This will only be meaningful if there are agreed minimum standards. These should, among other things, liability and further clarity to meet requirements. Critically, the implementation of these initiatives and recommendations is key.

General

13. **What, if any, additional issues relevant to consistency in the regulation and supervision of banks and non-banks in their provision of cross-border payment services should be considered in the report?**

    None that we have noted for the moment.

UK Finance

FSB: Recommendations for Regulating and Supervising Bank and Non-bank Payment Service Providers Offering Cross-border Payment Services

UK Finance response

September | 2024

Introduction and summary

UK Finance is the collective voice for the UK banking and finance industry.

Representing around 300 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation.

UK Finance welcomes the FSB's considerations to strengthen consistency in the regulation and supervision of banks and non-bank PSPs (NBPSPs) in providing cross-border payment services, in a way proportionate to the risks associated with such activities.

Our members are supportive of the FSB's efforts to harmonise and enhance the regulation and supervision of banks and NBPSPs in cross-border payments with the overarching approach of 'same activity, same risk, and same regulation' and, in this response, call for the need for a detailed and balanced approach that includes the following:

- avoiding unnecessary duplication for instance, in terms of reporting requirements;
- clearly defining roles and responsibilities of all relevant parties – supervisors, competent authorities, banks, non-banks and any underlying organisations such as payment schemes, FMIs and third-party service providers;
- managing risks effectively, and
- promoting a level playing field.

In our response to the FSB consultation, we point out key issues for FSB consideration including:

- **Activity-based vs. entity-based regulation**: UK Finance agrees with the FSB's distinction but stresses the need for flexibility to avoid unintended consequences.
- **Definition of payments**: We recommend including instant/fast payments and addressing the treatment of paper-based instruments like cheques for regulatory purposes. We would recommend an agile approach to reviewing the definition as the ecosystem continues to evolve.
- **Payment systems**: We point out potential issues with the FSB's definition, particularly regarding the distinction between schemes and infrastructure.

We also note the importance of the role of banks and NBPSPs:

- **Access to payment systems**: UK Finance notes ongoing efforts to improve NBPSPs' access to payment systems, highlighting initiatives in the UK and EU. However, some members have raised the issue of the potential risks of concentration and the systemic implications of NBPSPs relying on the same banking partners.
- **Supervision and risk**: We point out the importance of consistent supervision for NBPSPs and highlight the challenges NBPSPs face like de-banking and access to safeguarding accounts, as noted by some members

We noted that the FSB, working with international coordinating bodies, industry and stakeholders can address cross-border payment frictions and risks including those related to:

- **Fraud**: UK Finance calls for global cooperation to tackle fraud and improve the repatriation of criminally acquired funds. The response also highlights the importance of addressing fraud at its source, such as through online platforms.
- **Consumer protection**: We advocate for clarity in consumer protection, especially in cross-border payments, and call for harmonisation between jurisdictions to avoid regulatory gaps.
- **Emerging business models**: We are concerned about the potential risks associated with new payment models and stress the need for consistent application of regulations.

Our response to the consultation also sets out recommendations for regulatory and supervisory alignment including:

- **Principles for development:** While supportive of the FSB's principles, UK Finance highlights the challenges of implementing them consistently across jurisdictions.
- **Licensing and recognition**: We support the alignment of licensing regimes across jurisdictions to promote consistency and reduce barriers to cross-border payments.
- **Information sharing and cooperation**: We strongly believe that there is a need for transparent and effective cooperation between regulators to facilitate global standards and combat financial crime.

In summary, UK Finance stresses the importance of international cooperation, consistency, and clarity in the regulation and supervision of cross-border payment services to ensure financial stability, consumer protection, and a competitive market.

UK Finance response to FSB questions

FSB's consultation questions 1-4 on definitions contained in the FSB report

Our members welcome the fact that the global authorities and standard setting bodies have sought to collaborate, across regional regulators, to design and agree common standardised definitions.

Generally, the FSB has captured the role of banks and NBPSP accurately; however, below we set out further considerations and share examples from international jurisdictions:

Activity-based versus Entity-based regulation: We note that the definitions distinguish between activity-based regulation and entity-based regulation and that the FSB has acknowledged in the latter definition that *"Competent authorities may also adopt a hybrid approach that combines elements of both activity- and entity-based regulation depending on the nature of each jurisdiction's regulatory structure"*.

Increasingly we are seeing the authorities in the UK and elsewhere converging around the principle of "same activity, same risk, and same regulation". We are supportive of that as a broad concept, but the approach inevitably requires fine tuning when it comes to the detail of the specific issue, circumstances and application to ensure a proportional approach and to avoid unintended consequences.

Definition of payments: The FSB has stated that the proposed definition of payments is intended to *"cover all types of electronic funds transfers and instruments (e.g. cheques, credit transfers, direct debits, card payments, e-money)"*. We think it would make sense to add instant/fast payments to the list as this payment type is gaining increasing focus in the market and tends to be distinguished from 'standard' credit transfers. Historically, paper-based instruments such as cheques are sometimes treated differently from electronic payment types from a regulatory perspective. Any differentiation in treatment of any instrument, including emerging developments around digital currencies, needs to be made clear at the outset. We would recommend an agile approach to reviewing the definition as the ecosystem continues to evolve.

Definition of payment system: The FSB has defined the term "Payment System" as a *"set of instruments, procedures and rules for the transfer of funds between or among participants"* which is taken from the 'Principles for FMIs". There is a risk that such a definition may not sufficiently address scenarios where there is a clear

delineation between scheme and infrastructure, which in turn results in different roles and responsibilities.

For example, in the context of SEPA, there is a difference between: (1) the SEPA scheme rules managed by the European Payments Council in its role as SEPA scheme manager; and (2) SEPA-compliant Clearing and Settlement Mechanisms (such as EBA Clearing's STEP2, which has its own rules that align with those set by the scheme). Again, we would recommend that the definition is reviewed as the ecosystem evolves to align with the "same activity, same risk, same rule" principle.

We suggest that the Wolfsberg Group, association of 12 global banks which aims to develop frameworks and guidance for the management of financial crime risks, provides a good example in seeking the inclusion of the Payment Market Infrastructures as well as FMIs in the definitions as both are critical to solving for a number of the issues identified.

Market practices: in reviewing the definitions put forward in the report, the FSB may wish to consider the implications of market practices and conventions. For example, we note that the focus of the FSB's Recommendations is on retail payments. Traditionally, a distinction has tended to be made between Large Value Payment Systems (high value, low volume) and retail payment systems, which the FSB describes here as "high volume, low value transfers". We agree that it makes sense to differentiate between wholesale and retail payments however we question whether today it still makes sense to refer to value as part of the definition. For instance, in the UK, the Faster Payments System would be classified as a retail payment system, yet the scheme rules allow for a maximum transaction limit of £1 million.

It is important that the FSB continues to have an approach to harmonising international requirements, as set out above, that ensures that the ecosystem is regulated end to end. As the payments ecosystem continues to evolve, regulators will need to adopt an agile approach to the definitions ensuring that they are reviewed on a regular basis and incorporate emerging business models across the payments ecosystem. For example, it may be necessary to extend the scope to include support services in the future. Requirements will need to remain sufficiently detailed and clear to ensuring a level playing field where NBPSPs are subjected to similar regulation as banks, and key to this is fairness and resilience, and critically, protection of customers.

Section 1 question 5: The role of banks and non-banks in cross-border payments

The multiplicity of banks and NBPSPs operating in the payments landscape supports the diversity of business models, innovation, competition and, ultimately, choice for payment service users.

The FSB report provides a good overview of how the roles of bank and NBPSPs and their interrelationships have evolved and, here, we set out further considerations and provide examples.

NBPSP access to payment systems and accounts with central banks: The report makes reference to restrictions applying in *"most jurisdictions"* to NBPSPs' ability to access systemically important payment systems and maintain settlement accounts with central banks.

We note that these are areas of focus in the UK and European Union.

- For example, the Bank of England already permits NBPSPs to access RTGS and earlier this year issued a Discussion Paper on "Reviewing access to RTGS accounts".
- The European authorities have recently approved changes that are being introduced through the new Instant Payments Regulation, which are intended to improve NBPSPs' access to payment systems and give NBPSPs the option of safeguarding users' funds in an account held at a central bank where the latter (at its discretion) provides such a possibility. In July 2024, the European Central Bank published its Policy[1] in this regard. The policy allows NBPSPs established within the EEA access to all Euro area central bank-operated payment systems (not only TARGET) provided that all necessary risk-mitigation requirements are in place. However, a decision has been taken that Eurosystem central banks shall not offer safeguarding accounts to NBPSPs on the basis that this is not a core function for central banks and brings with it a range of risks which are detailed in the policy document.

1 https://www.ecb.europa.eu/paym/target/target-professional-use-documents-links/tips/shared/pdf/Eurosys_pol_on_access_to_central_bank_operated_payment_systems_by_NBPSPs.pdf

Direct versus indirect payment system access: An increasing number of jurisdictions are exploring forms of direct access for non-banks, with the US being the only G7 outlier. A recent CPMI survey also indicated that "jurisdictions that have expanded their access policy, particularly to NBPSPs, did not report major negative impact to the structure or operation of their payment systems. However, next to a growth in transaction volumes, several payment systems reported increased need for help desk support and a rise in operational incidents (including cyber-attacks) as an impact of a change in the composition of participants accessing the payment

system." This example showcases that some of the perceived risks that NBPSPs may pose to payment systems fail to materialise if the right mitigating measures and supervisory criteria are introduced.

Inevitably direct participation brings with it certain expectations and responsibilities, which are necessary to mitigate risks of failure to maintain mutual trust and financial stability. For instance, the first non-bank PSP given access to CHAPS in the UK, entered administration a year later, which emphasises the importance of ensuring that appropriate controls and preventative measures are in place to protect the integrity of the payment system and to avoid placing an increased or disproportionate risk on other participants

There should continue to be recognition that for some bank and NBPSPs direct participation may not be the ideal solution and they may prefer to participate indirectly. Accordingly, support for such arrangements should continue. We note the work done in the UK by the Payment Systems Regulator and at industry level to promote greater transparency on the part of sponsor banks to make it easier for indirect participants to compare service offerings. This is indicative of the positive role that competent authorities and industry associations can jointly play in facilitating broader awareness and understanding of the different options available.

Supervision for NBPSPs: Some of our members believe that as part of license applications and supervision, non-banks should consistently be assessed as part of BAU supervision. However, as non-banks still have to rely on banks for a large part of their operations, supervisors may be tempted to rely on the due diligence banks perform on their non-bank partners. While the due diligence of banks is always carries out to a high level, they may not have the full cross-market purview of a supervisor. This can lead to a knee-jerk reaction if something goes wrong and can result in an unnecessary clampdown, prohibiting or limiting certain business models or activities. In addition, in some countries providing cross-border payments or remittances are restricted for non-banks.

The requirements of supervisors sometimes mean that for some NBPSPs there is a risk of being de-banked across jurisdictions. Banks may be required to off-board NBPSPs or withdraw from servicing NBPSPs altogether as they seek to meet their

own compliance obligations. Some of our members view this as an inherent barrier to competition within the payments market. It also means that the customers of the NBPSP - as well as non-customer recipients - can lose access to a service they relied on from one day to the next, while the NBPSP looks for a different partner and needs to negotiate a new deal in a weaker position. Re-opening that service may come at an increased cost.

In addition to the risks surrounding non-bank access to payment accounts, the report rightly notes that non-banks also rely on banks to maintain segregated accounts for client funds with commercial banks or 'safeguarding' of customer funds. As non-banks grow in size, some members feel that there is increasingly less to no choice between providers with which they can safeguard their customer funds, especially when certain jurisdictions mandate having at least two safeguarding accounts. This leads to non-banks becoming increasingly clustered around a small number of banks that are large enough and have the risk appetite to hold billions in segregated customer funds. Some of our members believe that one approach would be enabling safeguarding at central banks as an additional option for non-banks, they would gain access to a broader range of diversification possibilities for safeguarding their customer funds. This is already possible in certain countries and helps reduce concentration risks, lower the risk profile of safeguarded funds, mitigate third party de-banking risks and increase consumer trust in safeguarded funds.

Diversity of payments business models: In the context of cross border payments, it is necessary to capture all firm types as there are long standing alternatives to banks, such as money transmission bureaus and Fintechs whose models eventually rely on traditional banking systems to move money. Managing the risk of these models is important.

A future view is also needed as big tech moves into the cross-border payment space and the consequences considered from a regulatory point of view. Consideration needs to be given as to how this model can be actively regulated to protect customers.

In addition, ACH to ACH models are emerging as ISO 20022 standards are adopted, and consideration should be given as to how to regulate and monitor these models too. The topic of regional models is interesting especially after failed attempts in the Nordic region (due to lack of agreement on the “Central Bank” for 5/6 currencies), but the successful implementation of BUNA in the Middle East is worth noting. Other initiatives, such as BIS Agorá should also be considered.

Payment mechanisms such as CBDC and digital currency are in active development globally on a regional and country basis, but it is unclear how they would work in a cross-border environment. It is important to consider whether the central banks need

to have agreements in place with each other to make global cross border payments more straight forward in the future whilst maintaining security and integrity.

Section 2 question 6: Cross Border Payment Frictions and Risks

Our members broadly agree with the risks and frictions caused by inconsistencies in the legal, regulatory and supervisory frameworks, and identified by the FSB. Here, we set out additional considerations:

Fraud: As the speed and ease of making a payment increases, this can make fraud and other economic crime easier to perpetrate. We encourage the FSB to consider ways in which regulators can collaborate internationally to establish ways for criminally acquired funds to be returned, confiscated or otherwise repatriated to appropriate authorities.

Different applications of global financial crime and fraud standards can create friction and credit risk in provision of cross border payments. An example would be recent issues some members have seen in applying a hold for cover parameters to inbound cross border payments, whereby straight-through-processing of inbound payments (rather than waiting for cover funds) has on a number of occasions seen some members out of pocket as the beneficiary bank, on the basis of differing application of localised financial crime policies through intermediary banks. Inconsistent application of AML/CFT regulation can impact on STP and cross-border settlement.

It is worth highlighting that the root causes of fraud can't be tackled by the financial services industry alone. It is crucial that the whole fraud chain is brought in to ensure higher levels of consumer protection and lower levels of fraud. For example, analysis in the UK shows that 70% of APP scams[2] started on an online platform, defined as emails, social media, websites (including auction sites), and apps (including dating apps). Often these are paid-for advertisements, meaning that social media companies are profiting from fraudulent ads while the finance sector bears the brunt of the cost. In many jurisdictions, there are live conversations around the inclusion of online platforms, including social media platforms, into any fraud mitigation response. Collectively, this would help tackle fraud at source instead of focusing solely on financial institutions as the last stage in the fraud value chain. We believe that this is a crucial and global step and would encourage the FSB to investigate a global coordinated response.

[2] https://www.ukfinance.org.uk/press/press-releases/over-two-thirds-of-all-app-scams-start-online-new-uk-finance-analysis

In addition, the FSB highlights that NBPSPs are more likely to engage in "occasional transactions" and while that may be true for some companies, it's worth highlighting that many NBPSPs tend to be younger companies, starting from the first fintech wave in 2010-2015. This means that they often don't have the same long-established client relationships to fall back on as banks do. While transaction monitoring is often paired with machine learning and AI to combat financial crime from taking place on their platforms, the lack of history can sometimes pose risks which could be addressed by stronger information sharing between the financial services industry. Financial crime remains a joint fight.

Consumer protection: The FSB report rightly references consumer protection as one of the risks. In developing measures designed to support or protect consumers, regulators should keep in mind that payments (whether domestic or cross-border) need to suit a range of needs and different types of users. Therefore, it should be borne in mind that some measures may be inappropriate or require re-configuration for the corporate space.

Domestic and international payment chains: In many jurisdictions, there is no mechanism to recognise that a domestic payment is part of a chain of a cross-border payment. Where local payment rails are used to send international transactions, payment infrastructure limitations can obstruct the inclusion of additional payer or payee data. Even if the additional information is included in the payment message, the information would not necessarily be captured by the recipient's financial institution because they would automatically classify it as domestic. We believe that this is an issue stemming from current payment infrastructure limitations rather than from specific payment business models, but it is an area where changes to domestic payment infrastructure could make a real difference to innovation in the processing of cross-border payments. This also has an impact on financial institutions' ability to apply the appropriate sanctions screening.

Scope of application of any requirements: There needs to be clarity on the scope and application of any associated legislative framework and, where appropriate, there should be an ability to apply a "corporate opt-out" – as is the case with the EU's Payment Services Directive.

ML/TF: The FSB paper usefully points out that: *"…while a jurisdiction's regulatory requirements for CDD and suspicious activity monitoring generally will apply to both banks and NBPSPs, the supervisory approaches for enforcing such compliance often vary, especially if the AML/CFT and prudential supervisors are different or if the jurisdiction does not require licensing of all non-banks PSPs. Since most NBPSPs currently access national payments systems through banking relationships, in those circumstances where the PSPs do not establish customer relationships that facilitate the conduct of effective CDD, the bank's exposure to ML/TF risk may be increased. Supervisors in turn may view those increased risks as not sufficiently mitigated by*

controls established under the bank's AML/CFT compliance programs." There needs to be a level playing field and it is not proportionate to expect banks to take responsibility for conducting CDD on their clients' clients.

Capital controls: there are inconsistencies in the application of "beneficiary verification", i.e. imposing verification on the end-beneficiary. This is generally overly burdensome. PSPs do not have relationships with the beneficiary. They are required to contact the recipient with insufficient contact data and go through the verification process before the payment can proceed in where they are not known to the recipient. This adds to the time and friction to the payment process.

Impact of emerging business models: Application of FATF Recommendation 16 is not universal, and it can be difficult for banks to police as payments landscapes evolve rapidly. We encourage the FSB to set out how national regulators can more consistently apply these requirements in line with the 'same activities, same risk, same regulation' principle.

It may be useful to consider adding further examples to the report. For example, Automated Clearing House (ACH) transfers where there is a lack of infrastructure to support compliance with requirements and leads to truncation of data could lead to inconsistent application of the rules, impeding effective monitoring and compliance with the Funds Transfer (Information on the Payer) Regulations.

While the FSB refers to FATF's R.16, it is worth noting that this was originally drafted with a correspondent banking model in mind, assuming that international transactions include routing of transaction messages via a centralised messaging system (such as Swift). In contrast, some companies facilitate cross-border payments by making two domestic transfers rather than going through the correspondent banking network.

Lack of harmonisation in licensing frameworks is detrimental for firms looking to operate cross-border. While certain countries have replicated frameworks that broadly mirror the UK/EU (with payment institution and e-money licenses), other jurisdictions still take a bank vs non-bank approach without recognising varying permissions in the non-bank framework. There is no "sliding scale". It is worth noting that introducing licensing regimes such as the UK and EU has also brought these non-banks into the regulatory framework of other legislation, such as rules around operational resilience. This is ultimately beneficial for the ecosystem as a whole.

Section 3 question 7: Principles for developing recommendations

The principles usefully highlight the importance of resilience, efficiency, proportionality, cooperation, coordination, and responsiveness to change.

While the principles are sensible, their interpretation in practice will require debate and widespread global understanding. For example, addressing issues such as how will proportionality play out in practice? Is there a risk of a lowest common denominator? Conversely will some parties use the cross-border principles to insist on practices required in their own jurisdiction to be used in other jurisdictions?

Thus, we see that though a more harmonised cross-border regulatory regime is desirable, it will be important that regulatory and supervisory bodies ensure on-going alignment is maintained. Any harmonisation must be proportionate to the perceived risks and must avoid gold plating and regulatory arbitrage. Alignment of regulatory regimes must be an enabler of cross-border payments, not introduce undue frictions. An example of potential overreach would be FATF's recent consultation on FATF Recommendation 16 which considered a potential requirement for receiving PSPs to verify payee details in the payment message against KYC details on file – a potentially material step change that could have a significant impact on STP for cross-border payments.

The complexity and challenges of these cross-border principles is only illustrated by the fact that we appreciate that there will from time to time be genuine reasons why particular states would have a need for local rules.

Section 4 questions 8-12: Recommendations for improving alignment of PSP regulatory and supervisory regimes.

We note that the six policy recommendations in the consultation report are directed at competent authorities who may be better placed to determine whether they are sufficiently granular, actionable, and flexible. They are helpful, however, in setting out areas competent authorities should consider from a cross-border payments perspective and providing a foundation to support greater consistency.

We also note that bridging the gap between recommendations and detail of national, legal and regulatory frameworks is going to be challenging unless there are agreements between specific regulators in different countries.

Recommendation 1

We welcome the fact that the stated intention under Recommendation 1 is to achieve "*a level-playing between bank and NBPSPs that reflects the principle of "same activity, same risk, same rule", while taking into account the differences in risk profiles"* and agree that this *"requires a comprehensive and sophisticated understanding of PSPs' activities and their risks as well as on potential mitigants to ensure the safety and efficiency of cross-border payment services"*. Such mitigants should also be proportionate and allocate responsibilities and expectations fairly between the parties.
We would appreciate further clarity on, for example, do Competent Authorities look only at PSPs registered in their jurisdiction and are they expected to allow others to operate in their territory? Also if there is a passporting regime in place.

Recommendation 2

The recommendation seeks to ensure consistency, but it is important to acknowledge that in some instances a one-size-fits-all approach may not be appropriate to accommodate the variety of business models in the market. The more informed competent authorities are - especially in the context of new, emerging products and services - the better, so engagement with industry will also be key to avoid misunderstandings and unintended consequences.

Recommendation 3

This recommendation could be more granular and actionable. It states that *"consumer protections should include ensuring transparency with respect to payment service delivery and pricing of services".* It could further refer to the G20 Cross-border payments roadmap goals, particularly on transparency of fees. Some members propose that this should include FX margins, which - to the FSB's own admission - make up a large proportion of the cost of a cross-border payment.

Our members would encourage the FSB to ensure that consumer protection requirements apply to both banks and NBPSPs. In addition, the FSB should further clarify targets and metrics regarding transparency on transfer pricing. This is currently falling by the wayside, with many jurisdictions focusing on speed disclosures or singling out upfront fees, while disregarding FX margins.

We also note that consumer protection shouldn't be a competent authority's' sole objective, giving the example of the FCA in the UK, whose operational objectives are to:

- protect consumers from bad conduct,
- protect the integrity of the UK financial system,
- promote effective competition in the interests of consumers.

Since 2023, the FCA has had a secondary objective to facilitate the international competitiveness and growth of the UK economy in the medium to long term (subject to alignment with international standards).

It is also important to consider implementation detail. For examples, how will consumers action their protections? In which jurisdiction will they have rights? Can they always go through their own PSP? How will that PSP secure resolution a miscreant in another jurisdiction?

To make these recommendations effective the FSB will need to secure agreement between many national authorities on how consumers can action their cross-border rights.

Recommendation 4

We support the idea that competent authorities should communicate clearly their expectations directly to the market and relevant parties (be they bank or NBPSPs or direct and indirect payment system participants). We also agree that the provision of *"dedicated assistance"* to PSPs (such as workshops) by competent authorities is welcome.

- From a UK perspective we have seen the benefits arising from publication of the Financial Conduct Authority's Payment Services Approach Document as a way of providing guidance.
- At EU level, recent workshops and subsequent publication of the European Commission's Clarification of requirements of the Instant Payments Regulation provides another example of an approach to promote consistent interpretation of text.

To further alignment and best practice, outputs from focus group discussions and supervisory practises must be shared, rather than encouraged, with other jurisdictions if consistency is to be a stated aim, although we expect this would be difficult achieve. There will be a requirement for a body to orchestrate and best practice is implemented. There is a potential gap in rules and responsibilities which may be filled by FSB issuing market guidance.

Recommendation 5

We are strongly supportive of Recommendation 5 as a way to promote a level playing field but also to provide a stronger basis for successful partnerships between banks and NBPSPs, for example in the context of payment facilitators for payments into wallets.

We note that the FSB states that Recommendation 5 *"focuses on domestic licensing"* and is asking *"How and to what extent would licensing recognition regimes between jurisdictions support the goal of strengthening consistency in the regulation and supervision of banks and non-banks in their provision of cross-border payment services?"* The more that licensing regimes are aligned, and firms are held to similar standards regardless of jurisdiction, the greater the level of consistency that can be achieved. This still runs the risk of competent authorities interpreting requirements in very different ways. This is where having global-level agreement on minimum requirements could prove beneficial
The huge success of the EU's licensing regime, which enables passporting of services across all countries in the EU cannot be overstated. It's evident by the sheer number of payment and e-money institutions offering their services across the EU's Single Market. This significantly benefits citizens from markets without major payments players of their own, as they can still reap the benefits of the services those PSPs offer when they might not have considered entering that market if passporting hadn't been available.

The EU's system of mutual recognition of licensing both within the EU and some third countries would be similarly beneficial if extended to other pairings of jurisdictions. For example, in a hypothetical scenario, a recognition agreement between UK and South Africa (SA) would give leeway for payments coming from SA and PSPs sending from SA that could be accepted into UK without such detailed checks.

Equivalent licencing regimes would support cross border payments, however, regulators would need to consider the liability of firms in one jurisdiction to firms in another on items such as consumer protection or errors made in payment processing.

It is not simply initial (and ongoing) alignment between payment licensing but also Wider societal change and best practice that may require ongoing alignment. There is also the question of how and to what extent would licensing recognition regimes between jurisdictions support the goal of strengthening consistency in the regulation and supervision of banks and non-banks in their provision of cross-border payment services? What risks need to be considered?

Recommendation 6

We strongly agree with the statement in the paper underlying Recommendation 6 that says that *"cooperative arrangements among regulators should be transparent to PSPs, other financial institutions and third parties so they can understand the regulatory environment and meet their customers' expectations and regulatory obligations, as well as consumers"*.
Relevant authorities should ensure that there is sufficient information sharing across jurisdictions, so 'host' states can increasingly rely on 'home' state requirements without introducing additional burdens that become barriers to expansion for PSPs operating globally or across borders. This includes data localisation requirements which are often burdensome, decrease operational resilience & data protection and add to financial pressures as they often lead to significant additional headcount. In addition, AML/CTF requirements should follow global rules and standards.

Policymakers will need to consider how financial institutions can share more information with competent authorities and with other industry participants within the relevant privacy frameworks. Today, these frameworks hamper the introduction of a strategy that would combat financial crime and fraud effectively. The fraud chain often starts online and today, online platforms and the financial services industry are unable to work together to tackle the root causes of these types of financial crime.

From a priority and effectiveness perspective, our members suggest that the focus for should be on facilitating the implementation of already agreed global standards and targets, such as those set out in the G20 Roadmap for enhancing cross-border payments.

As the proportion and value of payments sent via non-banks increases, in order to protect customers and ensure the stability of the system, comprehensive international standards for the regulation and oversight and supervision of banks and NBPSP will become essential. This will only be meaningful if there are agreed minimum standards. These should, among other things, liability and further clarity to meet requirements. Critically, the implementation of these initiatives and recommendations is key.