

January 8, 2021

By electronic submission to fsb@fsb.org

Secretariat to the Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland



Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships

The IIF and its members welcome the opportunity to respond to the FSB's discussion paper on the above topic.¹

The paper is timely given the ongoing work by the sectoral standard-setting bodies (SSBs)² and the growing importance of outsourced service providers and other third-party service providers (TPSPs), including the increased prominence of cloud service providers (CSPs) during the COVID-19 pandemic.

It also complements the current regulatory and supervisory focus on operational resilience within the financial sector, which aims to support financial stability and ensure proper functioning of markets to serve clients where they do business. TPSPs and outsourced functions therefore contribute to operational resilience of the system and themselves require a robust operational resilience approach.

Through the connection with cloud computing, the FSB's paper has a direct link to financial innovation. In the IIF's view, migration to cloud service provision by financial institutions (FIs) is a vital enabler in times of disruption, both by reinforcing operational continuity, thereby also bolstering operational resilience, and by supporting the digital transformation that is needed to meet enhanced customer expectations amid intensifying competition between incumbents and new entrants.³

Importantly, any proposed regulation and supervision therefore need to be carefully calibrated to avoid limiting the potential for innovation in this area. Ultimately, FIs themselves are best placed to determine how to embrace innovation in a way that both meets the desired outcome of regulations and is also relevant and proportionate to their unique business and risk profile. We would therefore encourage approaches to third parties and outsourcing that rely on firms' own risk management frameworks in the first instance and impose supervisory measures only if those frameworks are inadequate.

¹ FSB (2020), *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Discussion paper*.

² Such as work by IOSCO and the BCBS, building on the Joint Forum (2005), *Outsourcing in Financial Services*.

³ See IIF (2020), *Cloud Computing: A Vital Enabler in Times of Disruption*. See also the Future of Finance report commissioned by the Bank of England (2019), which stated at page 2: "Cloud technologies have matured to the point they can meet the high expectations of regulators and [FIs]. Shifting from in-house data storage and processing to cloud environments can speed up innovation, enable use of the best analytical tools, increase competition and build resilience".

Supervisors should be encouraged to adopt proportionate, risk-based, and outcomes-focused approaches to third-party arrangements, while fostering increased coordination between authorities to promote regulatory and supervisory harmonization.

Fragmented, unclear, and rapidly changing international standards and regional/national rules and guidance around outsourcing create uncertainty that impedes progress and innovation and impose a large cost and compliance burden on the regulated financial sector. There is scope for better alignment of concepts and terminologies, and also in the timing of initiatives, between geographies and across sectors.

FIs stand ready to partner with the official sector to come up with more innovative and more collaborative ways to monitor and manage risks arising from TPSPs, such as systemic risks that may arise from concentrations among TPSPs.

There may also be a need for a more ambitious compact among G20 countries to tackle issues such as data usage, data privacy, and data flows/data localization where fragmented or over-prescriptive rules often complicate outsourcing arrangements without commensurate benefits to end users, or to effective supervision.

In what follows, we answer questions 1 – 3 on a thematic basis, rather than repeat each theme under each question, and we answer question 4, on COVID-19 initial lessons learned, separately.

Q1. What do you consider the key challenges in identifying, managing and mitigating the risks relating to outsourcing and third-party relationships, including risks in sub-contractors and the broader supply chain?

Q2. What are possible ways to address these challenges and mitigate related risks? Are there any concerns with potential approaches that might increase risks, complexity or costs?

Q3. What are possible ways in which financial institutions, third-party service providers and supervisory authorities could collaborate to address these challenges on a cross-border basis?

A. Proportionality, risk-based and outcomes-focused supervisory approaches

Key challenges (Q1)

Members feel there can be a **lack of proportionality** in, or of risk-based supervision of, requirements relating to TPSPs, including CSPs.

Members report that supervision may prevent or hinder **intra-group outsourcing** arrangements between geographies, even if this would be not only more efficient, but also more effective at achieving operational resilience and risk management for the FI than fragmented operations.

Members have also noted that having full **exit strategies** for intra-group outsourcing arrangements would not be proportionate to the possible risks, or justifiable based on the business conducted in the respective jurisdictions. Such strategies may also be in conflict with objectives sought through recovery and resolution and ring-fencing rules. Emphasis on exit planning shifts the focus from resilience to replacement, when transitioning services during a business disruption may expose the FI and its customers to greater risk than ensuring effective recovery of services. Supervisors should be clear exit is a last resort.

Some supervisors also may focus more on new risks arising from **cloud migration** than on the operational risks of maintaining legacy technology stacks. Also, in some cases the risks of the FI losing competitiveness, and therefore financial resilience, against cloud-native challenger FIs or BigTech entrants may be profound. Cloud-tolerant or cloud-welcoming messages that are heard from senior regulators are not always consistently applied by supervisors or inspectors on the ground.

As another example, some regulators may impose “**multi-cloud**” requirements on FIs, whereby critical services are subject to failover arrangements to another CSP. Such prescriptive and subjective requirements may increase individual risk and/or increase cost and complexity to the FI, particularly if the requirements require failover installations to be “active-active.”⁴

Possible mitigants and concerns (Q2)

Supervisors should be encouraged to adopt **proportionate, risk-based, and outcomes-focused approaches** to third-party arrangements, including with regard to materiality and criticality definitions. These should be technology-neutral to ensure they are future-proof and applied equally across FIs, fintechs, BigTechs, and Financial Market Infrastructures (FMIs).

Regulators should be strongly encouraged to adopt an **outcomes-focused approach** which specifies the regulatory outcomes that regulators seek to achieve and provides FIs with the ability and flexibility to choose, in a principled and disciplined way, how to deliver that outcome.

Given that **intra-group outsourcing** on a cross-border basis can reduce overall risk while improving efficiency, supervisors should allow intra-group outsourcing, treat it differently than external outsourcing, and seek instead to ensure that the locally regulated legal entity is able to show that it is complying with the applicable local regulations and standards regardless of where the technology is located or risk management is carried out. Different treatment is justified because intra-group services are subject to well-controlled and globally consistent FI policies and processes, and those intra-group services which are compliant with recovery and resolution and ring-fencing rules have already met the intended outcomes of several third-party risk management requirements, including those around exit, business continuity planning, and sub-contracting. Protectionism or “data nationalism” should play no part in supervisory policy in this space.⁵

As for **cloud migration**, the security, operational and resiliency risks of *not* migrating to cloud as compared to retaining legacy systems that are static, and the resiliency benefits to FIs and the financial system of cloud computing more broadly, are significant.⁶ In order to support the safe migration to cloud by FIs, supervisors should continue to work with FIs and CSPs to appropriately understand cloud benefits and risks. In some cases, supervision would benefit from ensuring that messages about the desirability or acceptability of cloud migration delivered by their senior management are consistent with staff practices at the supervisor/examiner level.

We also believe that an arrangement with a TPSP should only be considered outsourcing if it is recurring or on an ongoing basis.⁷ Without this approach, there is a risk that a one-off or

⁴ Below, we make suggestions on how supervisors could monitor and address systemic risk aspects of CPS dependencies.

⁵ See further Section E below.

⁶ See IIF (2018), *Cloud Computing in the Financial Sector Part 1: An Essential Enabler*, and IIF (2020), *Cloud Computing: A Vital Enabler in Times of Disruption*.

⁷ This approach is taken by the European Banking Authority [Guidelines](#) on outsourcing.

single service could be subject to strict outsourcing requirements despite having a significantly reduced risk profile.

Possible cross-border collaboration (Q3)

Increased cooperation between FI supervisors in different jurisdictions could increase their willingness not to restrict intra-group or other outsourcing arrangements that cross borders. This could be developed through **cross-border supervisory fora** focused on risk issues arising from particular TPSPs or types of TPSP. Existing regulatory colleges or cooperative supervisory arrangements that might exist to oversee particular FIs, FMIs or other bodies such as SWIFT could be leveraged to discuss matters of mutual concern.

B. Regulatory fragmentation

Key challenges (Q1)

Firms active across geographies and sectors report **regulatory fragmentation** arising from different definitions of arrangements within scope of regulatory regimes targeted at outsourcing and third-party arrangements, including cloud.

There is a **lack of consistent definition** of terms such as outsourcing, third party relationships, information technology services, cloud services and the like, as well as a lack of consistency on thresholds or criteria for criticality/essentiality, material functions/outsourcing, and so on. Disparities amongst regulatory definitions and criteria lead to significant complexity, added cost and timing issues in implementing requirements in a global setting

Inclusions and exclusions from regulatory regimes are also inconsistent. For example, in some jurisdictions FMIs are within scope, while in others they are clearly excluded as being subject to their own regulatory regime which targets operational resilience.

Varying prescriptive approaches create a **fragmented picture of risk** and ultimately inhibit FIs and their supervisors from obtaining a consistent view of key areas of risk (including concentration risk) across jurisdictions or sectors.

FIs are also concerned about the possible cost implications for them and their end users of possible increased costs for TPSPs arising from **cross-sectoral resilience legislation**, especially if poorly coordinated with existing financial regulation.

Data standards around reporting of outsourcing and third-party arrangements and maintenance of outsourcing registers are similarly fragmented, and insecure manual systems of reporting predominate.

The substantive requirements for outsourcing (beyond terminology or reporting) are also not closely harmonized. For example, some members report a lack of consistency in expectations around **subcontractor** management, including in expectations on subcontracting chains through intra-group providers to TPSPs, where robust group processes and controls would be well established and executed.

Possible mitigants and concerns (Q2)

While concerned with the cost of complying with disparate regulations, members are also aware that any effort to harmonize or standardize regimes may lead to further regulatory change programs. Regulators should therefore be mindful that the one-off costs of such change programs may take a long time to amortize through lower ongoing costs, particularly if the timing of any changes is not coordinated.

One suggestion would be an exercise similar to the FSB’s Cyber Lexicon,⁸ which would **standardize terminology** largely by drawing on existing SSBs’ work, and which could be drawn upon in future standard-setting or regional/national rulemaking work.

If the **perimeter** of regulation is to be cast beyond outsourcing to third-party arrangements more broadly in a particular jurisdiction, care needs to be taken to ensure that the burden of supervisory and regulatory requirements is proportionate to the risk of the arrangements concerned. This means that an expansion into wider third-party relationships should be accompanied by a greater focus on more material or critical functions to ensure proportionality. An increase in scope, without a corresponding tailoring of requirements that apply to arrangements of differing level of risk, would be unworkable and inefficient.

The **relationship** between indirect regulation of TPSPs by financial regulators, and direct regulation by financial regulators (or by proposed horizontal digital resilience regulators in some jurisdictions) should be clear whenever new regulatory arrangements are articulated, and the cross-border implications should be clearly considered by the designers of such arrangements.

Ideally, **reporting** of third-party arrangements would become more standardized, digitized and secure, with **common data standards and APIs** becoming the norm.

Possible cross-border collaboration between FIs, service providers and supervisors (Q3)

Efforts could be made within the FSB to better **harmonize the overall principles** to be taken into account by sectoral SSBs in developing policies around TPSPs, including cloud.

In the absence of harmonization of detailed requirements across geographies, there should be more explicit reliance on **equivalence or substituted compliance decisions**, and more reliance placed on **home supervisor supervision**.

As pointed out by the FSB, global collaboration is needed to ensure that oversight contemplated is consistent and interoperable globally. As also mentioned in Section A above, **cross-border supervisory fora** or collaborative oversight mechanisms, similar to those that are in place for SWIFT and certain FMIs, may help to better align supervisory practices, at least in those jurisdictions where TPSPs are within scope of regulation.

Another approach could involve **closer coordination** at global and national levels between FIs, key TPSPs and supervisors to discuss matters and developments of mutual interest and to seek to agree standards or practical solutions. This is particularly the case regarding systemic risk arising from concentration which is unlikely be adequately addressed through regulation. We would encourage future private/public sector forums to consider these issues, as we have also suggested for operational resilience more widely.⁹

C. Audit processes and contractual or supervisory access to information

Key challenges (Q1)

Members have raised the fact that for some types of TPSP, such as CSPs, the same provider may be subject to dozens of (internal or external) audits on the same or similar topics, conducted on behalf of different FI clients seeking to comply with various regulatory or supervisory requirements. This is in addition to the self-certifications or third-party certifications that CSPs themselves may provide.

⁸ FSB (2018), *Cyber Lexicon*.

⁹ IIF (2020), *Response to BCBS Consultative Document on “Principles for Operational Resilience.”*

In some jurisdictions, including the EU and US, supervisors may also have rights to conduct their own inspections of TPSPs such as CSPs.¹⁰ For example, critical TPSPs are already required by some regulatory authorities to demonstrate robust operational risk management and operational resilience approaches to the FIs and authorities they support.

The result is that there appears to be significant **duplication** of effort between common clients and between supervisors, and therefore also significant scope to economize.

While some of the risks associated with the use of and reliance on unregulated third parties can be addressed through contractual negotiations, members report that some TPSPs are not willing to provide them with the appropriate **powers of access or audit** to enable them to comply readily with the requirements placed on them by FI supervisors. On their side, TPSPs (particular large CSPs or similar entities such as trade repositories) may feel that their own cyber security or operational integrity may be compromised by sharing and thereby possibly exposing highly sensitive information – including details of their cyber-defences – with multiple outside parties.

Members acknowledge the challenges with **subcontractor management**, particularly where there is a lengthy supply chain. An FI may have limited ability to contractually bind a subcontractor engaged by the FI's TPSP. Accordingly, it is also difficult for the FI to directly assess the operational resilience of that subcontractor and ensure parity of safeguarding measures.

Possible mitigants (Q2)

There may be actions the FSB can take to encourage legislators and regulators to facilitate **joint industry audits** or other collaborative reviews of TPSPs, to reduce the burden on FIs and TPSPs of duplicative information requests. Such audits have taken place successfully in recent years in Germany,¹¹ and anecdotally there are discussions to set up a special-purpose vehicle for this purpose in Australia. Data sharing, bank secrecy, liability and competition rules may all need to be reviewed to allow for this model to take place, including across jurisdictions.

As for **powers of audit**, the reluctance of some TPSPs, including CSPs, to share highly sensitive information about cyber defences could have a legitimate basis in their need to manage their own cyber risk, including legal risk as custodians of sensitive and valuable client data. However, if this is legitimate, the corollary is that FIs should not be expected to require this information. Instead, there may be scope for supervisors to **directly audit or supervise** these aspects of TPSPs.

The development of **certification schemes** would also be another way of attesting the capacity of these TPSPs to comply with the expected level of risk mitigation and resilience to supervisory authorities and FI customers alike. Such schemes could, potentially be based on internationally recognized standards such as those promulgated by the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), and other bodies, or related assessment tools based on such standards.¹²

¹⁰ Legislation such as the proposed *Digital Operational Resilience Act* in the EU, the *US Bank Service Company Act*, and Australia's draft Bill to broaden the *Security of Critical Infrastructure Act*.

¹¹ See BaFin (2020), [BaFin Perspectives 1](#) (in English) referring to the establishment by Deutsche Börse, of the Collaborative Cloud Audit Group (CCAG) in 2017. This industry-wide initiative, involving several major European financial institutions and insurance companies, was reported in 2020 to have conducted audits of global cloud providers such as Microsoft on behalf of its members.

¹² See e.g. [the Financial Services Sector Cybersecurity Profile \(FSP\)](#) launched by the IIF and other trade associations and housed at the Cyber Risk Institute.

Our members generally hold their suppliers contractually accountable for effective management of their **subcontractors** through contractual requirements. Any regulatory or supervisory expectations for FIs around subcontractors should be realistic and proportionate to the risks involved. For instance, the focus should be on critically outsourced (i.e., where the portion subcontracted is critical) arrangements, and to obtain assurance that they have robust third-party risk and supply chain frameworks.

Possible cross-border collaboration (Q3)

Mechanisms may need to be put in place to allow regulators in one jurisdiction to place reliance on joint industry audits undertaken in another, or to place reliance on audits conducted by supervisors in different jurisdictions.

As well, more engagement between TPSPs, audit firms, audit standard-setters, financial regulators and FIs could be helpful to clarify the content and nature of audits around specific topics such as cloud cyber security.

D. Systemic risk monitoring

Key challenges (Q1)

Many supervisors are concerned about what is perceived as a high level of concentration in some markets for third party services, especially cloud computing.

Some members consider that supervisors are also unclear in their definitions of concentration (and subsequently how this can be measured to establish systemic risk), as well as on the outcomes expected when a concentration is experienced.

While FIs are able to monitor the size of their own risk exposure to individual TPSPs, it is not their role, and some may not have access to the right information, to monitor risk concentrations at the system-wide level arising from multiple FIs' links to the same TPSPs.

There is also the challenge that direct supervisory oversight of CSPs could increase concentration by creating a situation where only the largest CSPs can absorb the costs of direct oversight.

Possible mitigants (Q2)

Given that FIs themselves do not have visibility into the precise third-party arrangements that other FIs maintain, there may be a role for supervisors to **map linkages between FIs and TPSPs**, particularly where there is a high degree of concentration among them. However, we caution that such information would itself represent a source of risk to the industry and to financial stability should it fall into the wrong hands, and any sharing or republication would need to carefully screen out information that is commercially sensitive. Given its sensitivity, supervisors would need to be very clear on the purpose of collecting and analysing such information.

It is also important that the public and private sectors work together to develop better ways to measure, monitor, and manage this risk; much remains to be done to gain better visibility into concentration risk within the system.

We believe that the right path forward is not to seek the elimination, drastic reduction, or even equal distribution of these risks; instead, the path forward should be focused on gaining visibility into concentration risk, building the right security and operational resiliency framework to manage these risks, and to work together deliberately and incrementally to create an environment which does not stifle the ability to utilize third parties.

Possible cross-border collaboration (Q3)

Consideration could also be given to providing the SSBs with a role in mapping concentration risk at the global level, similar to the work on Central Clearing Interdependencies that the FSB has undertaken in the past with the Basel Committee on Banking Supervision (BCBS), Committee on Payments and Market Infrastructures (CPMI), and International Organization of Securities Commissions (IOSCO). To this end, the FSB could engage closely with other SSBs and national authorities to consider the **interdependencies** across the global financial system and establish common policy outcomes sought across sectors.

The SSBs could also play a role in **system-wide stress test** scenarios with regard to TPSPs that may be considered systemic, in a similar conceptual vein to the supervisory stress testing of central counterparties.¹³ This would provide a more realistic, sectoral-wide result than stressing individual firms. Exercises that help all market participants better understand the actions they need to take and pre-identify risks that could arise would therefore be a useful initial step toward addressing concerns related to systemic concentration.

E. Data access and localization

Key challenges (Q1)

Data localization rules – i.e., rules which require data to be stored locally – impose costs and hurdles to the innovation process of internationally active FIs, without a commensurate increase in the achievement of regulatory objectives. Such rules create operational risk by necessitating localization of the technology needed to manage or store the data, and also restrict the provision of a range of services and innovation that are not commercially or technologically feasible under data localization rules. Additional technology results in more complexity and creates additional attack surface which must be defended. In addition, data localization rules have a detrimental impact on FIs' ability to fully leverage cloud and can lead to complex IT architecture and duplication in systems set-up, and potentially create new sources of information security risk.

Data nationalism, or clashes between regulators or between rules as to which regulators should be entitled to access data – for example, data about individual debtors or creditors which also constitute business records of the FI – can place FIs in a very difficult position vis-à-vis clients or supervisors. There are further significant challenges facing cross-border data transfers from the European Economic Area to third country jurisdictions in light of the *Schrems II decision* and subsequent changes proposed to transfers by the European Data Protection Board (EDPB).¹⁴

Possible mitigants (Q2)

Regulators should **avoid establishing data localization rules**, for the reasons mentioned.

Further, any direct access by supervisors to data held on behalf of FIs by CSPs should not be put in place in a way that risks compromising FIs' compliance with bank secrecy or data protection rules.

Resolution authorities should also consider the adequacy of their authority to enable supervisors/resolution authorities to keep TPSP contracts in force until resolution is

¹³ See CPMI and IOSCO (2018), *Framework for supervisory stress testing of central counterparties (CCPs)*.

¹⁴ In particular, there are aspects of the EDPB draft *recommendations* dated November 11, 2020 that could severely restrict the use of cloud service providers.

completed. Strengthening such authorities may be a viable alternative to requiring data to be held locally.

Possible cross-border collaboration (Q3)

The FSB could play a beneficial role in promoting **wider information-sharing** among regulators and supervisors to provide an alternative to, or reduce the adverse impacts of existing, data localization.

In the longer term, we suggest that **bank secrecy, data privacy and cross-border data flow rules may need to be more fully harmonized across major geographies and between sectors** in order to avoid FIs being subject to conflicting, divergent, or duplicative regulatory requirements (for example to maintain secrecy about customers resident in one geography while obliged to share data about those customers to regulators in another, where that data is also business records of the FI). This could be dealt with as part of the more ambitious compact among G20 countries we refer to in our general remarks.¹⁵

This is another area where greater reliance on home regulator supervision and cross-border collaboration between supervisors (e.g., supervisory colleges, collaboration agreements) should be explored.

Q4. What lessons have been learned from the COVID-19 pandemic regarding managing and mitigating risks relating to outsourcing and third-party relationships, including risks arising in sub-contractors and the broader supply chain?

Clearly, outsourcing of critical FI functions to the cloud, including mobile channels, has been a key enabler of resilience during the crisis, enabling widescale working from home, uninterrupted access to FI core systems, and the flexibility to quickly roll-out digital-only onboarding channels and “last-mile” solutions to deal with topics such as government subsidy distribution.¹⁶

As the COVID-19 pandemic has shown, FIs and supervisors must think of risks as global and not just business- or geography-specific.

Similarly, the COVID-19 pandemic has reinforced the need to plan for longer term recovery rather than only shorter duration/impact events.

FIs acknowledge the importance during periods like this of increased public/private collaboration.

Typically, a TPSP’s key performance indicators monitor the status of the services provided by the TPSP, but not of the status of the TPSP itself, such as the status of its infrastructure or key person risk.

Continuity planning has changed and further gained in importance (both for FIs and TPSPs themselves). Working from home is now a viable potential disaster recovery plan as opposed to reliance on off-site locations.

The COVID-19 pandemic has also illustrated the importance of the ongoing work internationally to monitor financial stability risks and to deliver effective operational resilience, as this would better prepare firms for future events where third parties are impacted

¹⁵ See page 2.

¹⁶ IIF (2020), *Cloud Computing: A Vital Enabler in Times of Disruption*.

on a large scale. Public authorities should consider how any additional requirements would sit alongside the developing regulatory approaches to operational resilience.

Cyber risk has escalated during the COVID-19 pandemic and has required strengthened cybersecurity measures to be implemented continuously during the pandemic. In particular, phishing and social engineering are widely used means of attack. Against this background, clear communication with service providers is particularly important as a preventive measure. Clear allocation of responsibilities in contractual agreements is key to make sure each side (FI and TPSP) understands the risks they assume, including configuration responsibilities.

The need for ‘stress testing’ using severe but plausible scenarios in partnership with third parties is increasingly important as, in today’s interconnected ecosystem, there will likely be multiple concurrent events and an increasing number of considerations that go beyond operational risks.

Looking forward, a flexible regulatory framework will be necessary, which does not prevent FIs from adopting advanced technologies in fields that are not closely linked to the execution of banking, insurance, asset management business, or other typically regulated financial services activities.

Economic and financial stress has been fast moving, affected suppliers indirectly through supply chain disruption, and has drawn certain small commodity providers not previously considered high risk into the category of operationally critical. In such turbulence the need to reassess the risk and sustainability of third parties frequently is crucial.

Nevertheless, although the COVID-19 experience is naturally top of authorities’ and firms’ minds, we think that managing and mitigating risk around third parties and outsourcing should be agnostic towards exact scenarios as we cannot predict the next material event.

Flexibility, principles- and risk-based and outcome-focused regulation is required to respond appropriately to a range of possible disruptions.

Conclusion

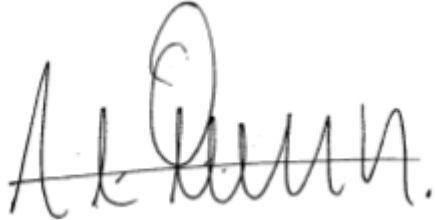
The IIF thanks the FSB for this opportunity to input and stands ready to engage in any stakeholder engagement process or interactive implementation process that is desired.

We, and our colleagues Laurence White (lwhite@iif.com) and Martin Boer (mboer@iif.com), would be happy to answer any questions or provide further details if required.

Yours sincerely,



Brad Carr
Managing Director, Digital Finance



Andrés Portilla
Managing Director, Regulatory Affairs