Electronic Money Association
68 Square Marie-Louise
Brussels 1000
Belgium
Telephone: +44 (0) 20 8399 2066
www.e-ma.org

Klaas Knot, President of De Nederlandsche Bank
Chairman
Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland

By email to fsb@fsb.org

22 August 2023

Dear Mr Knot

Re: Enhancing Third Party Risk Management and Oversight - Consultative document published on 22 June 2023

1. The EMA is the EU trade body of FinTech and BigTech firms engaging in the provision of a broad range of payment services and payment instruments. Our members include leading payments and e-commerce businesses issuing electronic money, providing online/mobile payments, card-based products, electronic vouchers, virtual currency exchanges, electronic marketplaces, merchant acquiring services and a range of other innovative payment-related business activities. Most EMA members operate across the EU and globally on a cross border basis. A list of current EMA members is provided at the end of this document.

2. We very much welcome the opportunity to respond to the FSB's Consultative Paper (CP) introducing a Toolkit for financial institutions and financial authorities to enhance third party risk management (TPRM) and oversight. EMA members use a range of outsourcing arrangements (external, intra-group) to deliver regulated services and are already required to manage effectively risks arising from the use of outsourcers. A

range of existing regulatory texts[1] detail risk management requirements related to the use of third-party service providers by financial institutions. Financial institutions are also already required to monitor major incidents (operational, cybersecurity, operational resilience) and submit reports to the relevant national competent authorities. In this context, financial industry participants are keen to avoid confusion and duplication of effort in their compliance assessment and reporting arrangements across different regulatory frameworks. Thus, it is important to seek (a) Consistency of relevant Terms across different regulatory frameworks and (b) Alignment of monitoring and reporting requirements across different regulatory frameworks.

3. Many financial institutions have very limited visibility of *nth-party service* providers that offer services to their outsourcers; such providers often offer ICT services to such outsourcers through intermediaries and VARs and are not even listed as (Critical) sub-contractors in outsourcing service level agreements. The power differential in many outsourcing relationships established by financial institutions makes it very difficult to receive information on the entire supply chain of large outsourcers to include in a Register of Information. In this context, we would encourage financial authorities to take on a more active role in engaging with systemic Critical outsourcers and impress upon them the need to identity Critical sub-outsourcers in their supply chain. The EU Oversight Framework - established to oversee Critical ICT third party service providers under the DORA Regulation - provides a mechanism that EU financial regulators can use to encourage such service providers to offer more information on all supply chain outsourcers that support the operations of financial institutions.

4. Building on the comment above, financial institutions are also not best placed to identify systemic third-party dependencies since they have limited visibility of the scope/reach of outsourcers' relationships across markets. We encourage the FSB to promote systematic communication across financial service regulators to identify such systemic, industry-wide dependencies and to share such information with financial industry participants. Authorities can leverage a range of outsourcing data reported by financial institutions to identify such dependencies across different industry segments and national markets.

5. The remainder of this note provides comments on some of the questions put forward in the CP.

Question 1: Are the definitions in the consultative document sufficiently clear and easily understood? Are there any important Terms and Definitions that should be included or amended?

[1] EBA Guidelines on Outsourcing Arrangements (EBA/GL/2019/02), EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04), EC Digital Operational Resilience Act (DORA), UK Operational resilience: Critical Third Parties to the UK Financial Sector.

6. The Terms listed in the *Common Terms and Definitions* section of the CP are mostly clear and well understood.

7. It would be useful to clarify the reference to a "*formal arrangement*" in the definition of ***third-party service relationship***. Specifically, clarify whether the reference relates to the existence of a standalone service delivery agreement detailing the services delivered to a financial institution through the relationship. We note that the delivery of services by entities that form part of the same group of companies as the financial institution may not always be documented in a separate service delivery agreement.

8. We would also encourage the FSB to clarify further the set of services that fall outside the definition of third-party service relationships. Specifically, clarify whether transaction processing services (*Card Issuer Processor, Card Acquirer Processor*) and technology services offered by regulated/non-regulated entities to enable subsequent financial transactions (*Payment initiation service providers-PISPs, account information service providers-TPPs, payment account access aggregators, digital wallet providers*) constitute third-party service relationships.

Question 3. Is the toolkit's focus on regulatory interoperability appropriate? Are there existing or potential issues of regulatory fragmentation that should be particularly addressed?

9. The focus of the CP on regulatory interoperability is appropriate and necessary. Our members are already required to track risks related to 3rd party service relationships according to a number of national and international regulatory frameworks. Any effort to introduce a new toolkit to enhance the ability of financial institutions to manage Third-party risk must aim to be interoperable with existing regulatory frameworks. The visibility (and treatment of risks related to the use) of Critical [Nth]-party service providers is likely to diverge across different jurisdictions depending on the approach adopted by the relevant financial services regulator.

Question 4. Is the discussion on proportionality clear?

10. The discussion on Proportionality in the CP is useful and appropriate. We would encourage expanding the discussion further to acknowledge differences in the ability of financial institutions of varying operational size to (i) Exit Critical third-party service relationships quickly with minimal service delivery impact, (ii) Negotiate access to cybersecurity and business continuity management documents of large Critical outsourcers as part of the due-diligence and service monitoring process and (iii) Mitigate third-party service concentration risks. Financial institutions with a smaller operational footprint and fewer resources should not be expected to adopt the risk management and mitigation controls of larger institutions on these issues.

Question 5. Is the focus on critical services and critical service providers appropriate and useful? Does the toolkit provide sufficient tools for financial institutions to identify critical services? Do these tools rightly balance consistency and flexibility?

11. The focus on Critical services on the service providers that deliver them to financial institutions is appropriate. The high-level criteria (In Section 3.1 of the CP) that may be used to identify a Critical service are useful. We would encourage the FSB to limit the scope of the concentration risk management principles (listed in Section 3.8 of the CP) to Critical 3rd party services. Such an approach aligns with the principle of Proportionality that the FSB has adopted in the CP.

Question 7. What are the potential merits, challenges and practical feasibility of greater harmonisation of the data in financial institutions' registers of third-party service relationships?

12. The contents of the Registers of 3rd party service relationships - maintained by financial institutions– can help financial services regulators identify Critical outsourcers that create systemic dependencies for the financial services industry. It is important to maintain the quality and consistency of the data stored in Registers of 3rd party service relationships. We note the suggestion to use unique Legal Entity Identifiers (LEIs) to identify outsourcers where these are available. The subsidiaries of some outsourcers or intragroup outsourcers may not always be assigned a unique separate LEI. As noted earlier, it will also prove difficult to identify [Nth]-party service providers in these Registers. Some of these service providers may not have direct service delivery relationships with Critical Outsourcers of financial institutions. Thus, the identification Critical Supply Chain service providers will prove problematic and impact the ability of financial institutions/authorities to identify such service providers in their Register of 3rd party service relationships.

Question 8. Are the tools appropriate and proportionate to manage supply chain risks? Are there any other actionable, effective and proportionate tools based on best practices that financial institutions could leverage? Are there any other challenges not identified in the toolkit?

13. As commented above, we perceive that financial institutions may have limited ability to identify all supply chain Critical outsourcers due to the lack of a direct relationship and the complex/fragmented supply chains used by a number of outsourcers. We encourage the financial regulators' community to support the efforts of financial institutions to identify critical supply chain outsourcers. Regulators can leverage a range of data (*major incident reports, registers of outsourcing arrangements, Operational Resilience framework data*) to identify such outsourcers and to flag Critical Supply chain outsourcers for the benefit of the financial services' industry.

Question 10. How can financial institutions effectively identify and manage concentration and related risks at the individual institution level? Are there any additional tools or effective practices that the toolkit could consider?

14. The concept of concentration risk on 3rd party service relationships often clashes with an outsourcing company's objective to limit its outsourcing relationships to a few, reputable suppliers to benefit from economies of scale/volume and streamline its outsourcing service monitoring and risk management processes. Some financial institutions outsource the majority of their outsourced services to a single intragroup outsourcer (a parent or sister corporate entity) that then takes on the task of managing 3rd party service relationships on behalf of the financial institution. In either case, it can prove problematic to mitigate concentration risk for 3rd party service relationships. We encourage the FSB to consider the intragroup outsourcing arrangement outlined above as it puts forward recommendations on managing concentration risk at an individual financial institution level. We would also put forward the presence of a credible Exit Strategy as an appropriate risk mitigation control to address increased concentration risk in 3rd party service relationships. Finally, we perceive that it would be more useful to consider 3rd party service relationship concentration risks at the level of local/national groups of financial institutions (as detected by financial authorities) rather than at the level of individual financial institutions.

Question 11. Are there practical issues with financial institutions' third-party risk management that have not been fully considered?

15. As noted above, we perceive practical difficulties in mapping the full supply chain of financial institutions and in identifying Critical [Nth] – party outsourcers that may not even have direct relationships with identified external/intragroup outsourcers. We encourage the FSB and financial authorities to support the efforts of financial institutions by (i) Sharing information with financial services' industry participants on Critical supply chain outsourcers they have identified leveraging existing incident/cybersecurity and operational resilience data and (ii) Engaging with Systemic Critical outsourcers to highlight the importance of identifying supply chain outsourcers that support the operations of financial institutions.

Members of the EMA, as of August 2023

AAVE LIMITED
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
Amazon
American Express
ArcaPay UAB
Banked
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network EMEA Limited
Boku Inc
Booking Holdings Financial Services International Limited
BVNK
CashFlows
Checkout Ltd
Circle
Citadel Commerce UK Ltd
Contis
Corner Banca SA
Crypto.com
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
emerchantpay Group Ltd
Etsy Ireland UC
Euronet Worldwide Inc
Facebook Payments International Ltd
Financial House Limited
First Rate Exchange Services
FIS
Flex-e-card
Flywire
Gemini
Globepay Limited
GoCardless Ltd
Google Payment Ltd
HUBUC
IDT Financial Services Limited
Imagor SA
Ixaris Systems Ltd
J. P. Morgan Mobility Payments Solutions S. A.
Modulr Finance Limited
MONAVATE
MONETLEY LTD
Moneyhub Financial Technology Ltd
Moorwand
MuchBetter
myPOS Payments Ltd
Nuvei Financial Services Ltd
OFX
OKG Payment Services Ltd
OKTO
One Money Mail Ltd
OpenPayd
Own.Solutions
Park Card Services Limited
Paymentsense Limited
Paynt
Payoneer Europe Limited
PayPal Europe Ltd
Paysafe Group
Paysend EU DAC
Plaid
PPRO Financial Ltd
PPS
Ramp Swaps Ltd
Remitly
Revolut
Ripple
Securiclick Limited
Segpay

Skrill Limited
Soldo Financial Services Ireland DAC
Square
Stripe
SumUp Limited
Swile Payment
Syspay Ltd
Transact Payments Limited
TransferMate Global Payments
TrueLayer Limited
Trustly Group AB
Uber BV
VallettaPay
Vitesse PSP Ltd
Viva Payments SA
Weavr Limited
WEX Europe UK Limited
Wise
WorldFirst
Worldpay
Yapily Ltd