Electronic Money Association
Crescent House
5 The Crescent
Surbiton
Surrey
KT6 4BN
United Kingdom
Telephone: +44 (0) 20 8399 2066
Facsimile: +44 (0) 870 762 5063
www.e-ma.org

Governance & Professionalism Policy
Strategy & Competition
Financial Conduct Authority
12 Endeavour Square
London E20 1JN
UK

1 October 2020

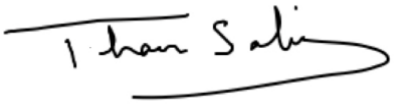
Dear Sir/Madam

Re: EMA response to FCA Consultation Paper 19/32 on Building operational resilience: impact tolerances for important business services

The EMA is the UK and EU trade body representing electronic money issuers and alternative payment service providers. We have over 70 members including leading payments and e-commerce businesses worldwide that provide online payments, card-based products, electronic vouchers and mobile payment instruments. A list of current EMA members is provided at the end of this document.

I would be grateful for your consideration of our concerns.

Yours faithfully



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

EMA response to consultation

Q1: Do you agree with our proposal for firms to identify their important business services? If not, please explain why.

The EMA agrees that it is important for firms to identify important business functions and assets/processes that support these functions. EMA members are already required to identify Critical/Important functions to track ICT and security risks that impact them[1] including outsourcing risk[2]. A clear and comprehensive definition of Critical/Important functions is already provided in Par. 29 of the *EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)*; we would encourage the FCA to reuse this definition.

Q2: Do you agree with our proposed guidance on identifying important business services? Are there any other factors for firms to consider?

The FCA guidance on identifying important business services (*as detailed in Chapter 4 of the CP*) includes a level of ambiguity that will increase uncertainty and introduce inconsistency in firms' processes of identifying important business services. Individual financial service firms are not necessarily best placed to assess whether a disruption to one of their services will cause intolerable levels of harm to UK market integrity. The systemic importance of the service(s) delivered by any single financial service institution is easier to assess from the perspective of the relevant competent authority; as an example, this is the approach already adopted by the control framework deployed to support the NIS Directive[3].

We agree that the publication of a prescriptive taxonomy of important business services by the FCA would be counterproductive.

We would request that the FCA provide more clarity on:

- The reference to a *clearly identifiable separate service* "*and not a collection of services*" in Par. 4.20 of the CP.

[1] As required in the EBA Guidelines on ICT and security risks (EBA/GL/2019/ 04)
[2] As required in the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/ 02)
[3] Directive (EU) 2016/1148

- The approach that can be adopted by small/medium size financial service providers in identifying important business functions in light of the guidance listed in Par. 4.21(a) of the CP that references the size of the customer base that is impacted.

Q3: Do you agree with our proposals for firms to set impact tolerances? If not, please explain why.

EMA members are ambiguous whether the introduction of Impact Tolerances will necessarily lead to fewer disruptions in the delivery of financial services to UK consumers. Our members are already required to perform regular Business Impact Analysis (BIA) assessments and to establish a range of recovery objectives (RTO/RPO[4]) for all Critical/Important functions. These objectives drive the business continuity planning process of financial service providers including testing, resource allocation/investment and management of outsourcing arrangements. In this context, the introduction of a new set of metrics (Impact Tolerances) can add further complexity and duplication to the firms' business continuity planning process.

Additionally, the guidance that is provided on setting Impact tolerances is ambiguous and confusing in a number of areas:

- The reference to seasonal peaks in Par. 5.11 of the CP.
- The mixing of quantitative/hard parameters (financial loss to consumers/firm) and qualitative/soft parameters (reputational damage, impact to consumer/market confidence) in Par. 5.12 of the CP. The use of qualitative parameters to set such Tolerances can prove especially problematic.
- The statement that the FCA "*do not expect firms to set their tolerances at excessively high levels*" in Par. 5.16 of the CP.

Overall, we believe that the existing industry use of recovery objectives (RTO/RPO) is effective in improving the business continuity capabilities of UK financial service institutions.

[4] Recovery Time Objective-RTO, Recovery Point Objective-RPO

Q4: **Do you agree that duration (time) should always be used as 1 of the metrics in setting impact tolerances? Are there any other metrics that should also be mandatory?**

Acknowledging our concerns on the benefits of establishing Impact Tolerances stated above, we note that the duration of unavailability of a service (Time to recover) is already one of the service recovery metrics that is currently used as part of the business continuity management process of UK financial service firms[5].

However, there are a number of other parameters that may be used to identify business continuity objectives (data volume, transaction/account volume, financial cost, customer numbers impacted). Financial service firms currently use the appropriate parameters to set such objectives to reflect their business and service delivery models. In this context, we encourage the FCA to continue to allow financial service firms to set their business continuity objectives without prescribing the use of any single parameter; this approach aligns with the principle stated in Par. 5.7 of the CP.

Q5: **Do you agree with our proposal for dual-regulated firms to set up to 2 impact tolerances and solo-regulated firms to set 1 impact tolerance per important business service?**

We understand the rationale behind the approach adopted by the FCA in proposing the establishment of two (2) impact tolerances for dual-regulated firms.

We invite the FCA and PRA to provide further clarity on the process they will adopt to monitor compliance with different operational resilience objectives set by dual-regulated firms.

Q6: **Do you have any comments on our proposed transitional arrangements?**

We support the establishment of a transitional arrangement of appropriate length to allow firms to align with new operational resilience requirements. We invite the FCA to provide further clarity on its expectations of:

[5] Recovery Point Objective-RPO.

- Firms setting and sharing their operational resilience objectives after the final FCA Proposal has been published and,
- Firms' services aligning with identified operational resilience objectives after the latter have been set. We note that the CP includes a rather vague reference to alignment as "*soon as practically reasonable*" and to the systemic importance of a firm[6].

Finally, we encourage the FCA to consider affording adequate flexibility to firms authorised during the transition period to align with any Operational Resilience framework depending on their size and systemic importance. Such an approach can ensure that the UK remains a preferred destination for the launch of small, innovative financial service providers.

Q7: Do you agree with our proposed approach to mapping? If not, please explain why.

We agree that it is appropriate for firms to identify underlying resources and assets that support the delivery of Important business services as part of a business continuity/operational resilience management framework.

We want to highlight that such mapping is a highly dynamic process; therefore, the FCA expectation that the output of the mapping process will be "*signed-off at an appropriate level by management*"[7] may prove difficult to meet in practice.

Q8: Do you agree with our proposed approach to testing? If not, please explain why.

We would challenge the value-add delivered by the approach to operational resilience testing outlined in Par. 6.8-6.17 of the CP. The extensive references to "*severe but plausible scenarios*" introduce ambiguity that will complicate the operational resilience testing of financial service firms.

The advice provided to firms in the CP on the process of identifying appropriate testing scenarios appears to point to the destructive testing processes adopted by other

[6] See CP Par. 5.24

[7] See CP Par. 6.4

industries[8]. It is not clear to us that the use of such extreme testing scenarios - that are extremely unlikely to occur or whose occurrence is often beyond the control of regulated firms – offers any actionable inputs to the operational resilience planning process of regulated firms.

Firms have already invested in limiting the likelihood of occurrence and service delivery impact of more extreme business continuity events. We would encourage the FCA to consider the effect of such investments in its expectations for operational resilience scenario testing by firms it supervises.

We want to highlight that the guidance provided in designing operational resilience testing scenarios in Par 6.15 of the CP does not include any reference to data availability. Access to such data is currently the focus of business continuity planning of many financial service firms as malicious software (ransomware) continues to target the industry.

Finally, we are concerned about the assertion made in Par. 6.16 of the CP[9] that appears to pre-judge the importance of service integrity vs availability as parameters of a testing process. The relative importance of such parameters is entirely dependent on the characteristics of the underlying Important business service (e.g. telecoms/IP/electricity grid access, network connectivity/security etc.). We invite the FCA to extend firms flexibility in identifying appropriate operational resilience test scenarios to reflect the characteristics of their service(s).

Q9: **Do you agree with our proposals for communication plans? If not, please explain why.**

We agree with the FCA proposals that firms establish communication plans as part of their operational resilience planning process. We note that financial services firms are already required to have established internal/external-facing communication plans under the *EBA Guidelines on ICT and security risk management*[10].

[8] Engineering, Energy, Transport

[9] 4th bullet point

[10] Guidelines 3.7.5 and 3.8

Q10: **Do you have any comments on our proposed requirement for a self-assessment document?**

We note that the generation and update of a self-assessment document that includes the detail listed in Par. 6.16 of the CP will require the allocation of significant resources by regulated firms.

We are concerned that the Outsourcing-related expectations detailed in the CP[11] do not reflect the power dynamic in the current relationships between regulated firms and certain types of outsourcers (e.g. cloud-hosting providers, payment processors/gateways). Additionally, the substitutability of such services is often limited and the transition from one provider to another costly and lengthy. Finally, many of these outsourcers are global entities and are not subject to any financial services regulation. In the absence of intervention by regulators, the ability of many regulated firms to identify/deploy controls to address operational resilience incidents related to the delivery of the services of certain types of outsourcers will continue to be limited.

We encourage the FCA to continue to apply the principle of Proportionality in its assessment of the level of detail included in operational resilience self-assessment documents created by firms of different size and scope of activities.

The EMA support the proposed FCA approach to avoid including the self-assessment document in the list of documents/reports that are exchanged with the FCA on a standardised annual basis.

Q11: Do you have any comments on the cost benefit analysis?

We have a number of concerns on the accuracy of the Cost Benefit Analysis (CBA) presented in Annex 2 of the CP:

- It is not clear to us how respondents to the industry Survey (and the FCA) can assess the additional benefits that the proposed operational resilience framework may deliver over the existing/baseline regulatory compliance

[11] Section 8

framework when a number of components of the baseline framework only started to apply in the last 12 months[12].

- There is uneven firm type representation in the set of respondents to the FCA Industry Survey that drove the CBA as indicated in Par. 33-Table 1 of the Annex. Specifically, we note that c.5% of authorised Medium/EMIs/ PIs/RAISPs responded to the Survey vs. c24% of the Large firms.
- The use of averages to calculate firms' costs of alignment with the proposed operational resilience framework[13] and the cost of operational resilience incidents[14]
- The current ambiguity of a number of the parameters of the proposed operational resilience framework (e.g. service identification, scope of scenario testing) make it even more challenging to come up with dependable cost/effort estimates
- The lack of any obvious consideration of the impact to existing outsourcing arrangements caused by the Outsourcing requirements in Section 8 of the CP.
- The piecemeal reference to a move away from a "*traditional risk management approach, towards treating disruption to business services as though it were inevitable*" in Par. 65 of Annex 2 of the CP[15]. The cost/impact of such a move to regulated firms will be very significant.
- The assertion that the adoption of the proposed operational resilience framework "*will allow firms to identify ways in which they can avoid disruption altogether*" in Par. 69 of Annex 2 of the CP.

Overall, we are concerned that the CBA underestimates the costs and overestimates the potential benefits of the introduction of the proposed operational resilience framework to UK firms.

Q12: Do you have any comments on the examples of existing legislation?

[12] The EBA Guidelines on ICT and security risk management started to apply on the 30th June 2020; the EBA Guidelines on outsourcing arrangements started to apply on the 30th September 2019.

[13] Par. 46 of Annex 2 of the CP

[14] Par. 43 of Annex 2 of the CP

[15] 2nd bullet point

We encourage the FCA to:

- Clarify to industry its intention to adopt the *EBA Guidelines on ICT and security risk management (EBA/GL/2019/04)* as a replacement for the earlier *EBA Guidelines on security measures for security and operational risks (EBA/GL/2017/17)*.
- Consider the operational resilience impact of the requirements introduced in the *EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)* as part of its assessment of the Baseline regulatory framework that informs its Cost-Benefit Analysis.
- Clarify the applicability of the operational resilience framework requirements to EEA-firms that enter the Temporary Permissions Regime (TPR), post-Brexit.

List of EMA members as of September 2020:

AAVE LIMITED
Account Technologies
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
American Express
Azimo Limited
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Ceevo
Circle
Citadel Commerce UK Ltd
Coinbase
Contis
Corner Banca SA
Crypto.com
Curve
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
Euronet Worldwide Inc
Facebook Payments International Ltd
First Rate Exchange Services Flex-e-card
Flywire
Gemini
Globepay Limited
GoCardless Ltd
Google Payment Ltd
IDT Financial Services Limited Imagor SA
Ixaris Systems Ltd
Modulr FS Europe Limited Moneyhub Financial Technology Ltd MuchBetter
myPOS Europe Limited
Nvayo Limited
OFX
OKTO
One Money Mail Ltd
OpenPayd
Optal
Own.Solutions
Park Card Services Limited
Paydoo Payments UAB Paymentsense
Payoneer
PayPal Europe Ltd
Paysafe Group
Plaid
PPRO Financial Ltd
PPS
Remitly
Revolut
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Soldo Financial Services Ireland DAC
Stripe
SumUp Limited
Syspay Ltd
Token.io
Transact Payments Limited
TransferMate Global Payments
TransferWise Ltd
TrueLayer Limited
Trustly Group AB
Uber BV
Vitesse PSP Ltd
Viva Payments SA
WEX Europe UK Limited
Wirecard AG
Wirex Limited
WorldFirst
Worldpay UK Limited
WorldRemit