Electronic Money Association
68 Square Marie-Louise
Brussels 1000
Belgium
www.e-ma.org

Consultation Paper 140
GOR
Central Bank of Ireland
PO Box 559
Dublin 1

Opresilience@centralbank.ie

9 July 2021

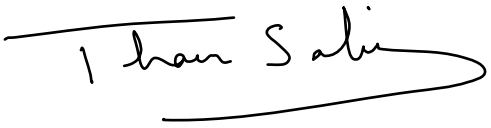
Dear Gabriel

Re: EMA response to CBI CP140 on Cross Industry Guidance on Operational Resilience

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide, providing online payments, card-based products, electronic vouchers, and mobile payment instruments. Most members operate across the EU, most frequently on a cross-border basis, and a large number have obtained – or are applying for - licences to operate from the Central Bank of Ireland. A list of current EMA members is provided at the end of this document.

I would be grateful for your consideration of our comments and proposals.

Yours sincerely,



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

EMA response

Consultation Questions	
Do the guidelines include the main elements that are necessary for an effective operational resilience approach for a firm?	EMA Ireland view the *Central Bank Cross Industry Guidance on Operational Resilience* as addressing the core elements of an operational resilience framework that regulated financial service providers will be expected to establish.
What, if any, are the other areas that should be covered in the proposals or in future guidance?	Operational resilience areas that may be covered in future central bank guidance could include: ▪ Criteria to use to designate Critical/Important business services (Guideline 3), ▪ Assessment criteria of the Impact Tolerances identified for Critical/Important business services (Guideline 5), ▪ Design of severe, plausible test scenarios to exercise Critical/Important business services (Guideline 10).
With reference to specific sections, what other significant factors or examples could be included in the proposals?	See comment above.
Are any parts of the guidance unclear or ambiguous?	It is not clear to us what evidence the central bank expects regulated financial service providers (RFSPs) to provide to demonstrate readiness to apply the guidance "*at the latest within two years of its being issued*" (*Implementation Section of Consultation Paper 140 –* ***CP 140***)? We invite the central bank to clarify further its expectations of regulated financial service providers on this topic.

	Separately, we note the central bank's statement that it will use supervisory engagement to assess alignment with core principles of operational resilience across firms including through assessing "*the firm's consideration of third parties in its response and recovery processes and that they are aligned and tested for effectiveness*." We invite the central banks to provide further clarity on the scope of RFSP involvement in testing the operational resilience arrangements of 3rd parties.
Are there any specific lessons resulting from the COVID-19 pandemic, including relevant containment measures, that the proposed guidance for operational resilience should reflect?	We want to highlight the importance of (i) operational flexibility, of (ii) re-configurable service delivery architectures, and of (iii) evolving cybersecurity requirements' frameworks in addressing the challenges introduced by the pandemic. The central bank cross industry guidance on operational resilience should seek to enhance the ability of RFSPs to incorporate these attributes into the design of their future products and services.
What are the significant issues /or concerns or unintended consequences that might arise due to the content of the proposals?	EMA Ireland perceive that the proposed cross-industry guidance may lead to: ▪ Disruption to the existing outsourced service delivery arrangements of most RFSPs, ▪ Duplication of effort for RFSPs that are supervised by the central bank that are also present in other national markets where other operational resilience frameworks are in force (e.g. the UK) or under consideration by the national competent authorities (e.g. the DORA regulation in the EU) ,

	▪ Introduction of additional operational complexity for all RFSPs; small/medium size RFSPs will experience a more significant impact.

Identify & Prepare	
Governance	We note the numerous references to ***Board*** responsibilities for the Operational Resilience framework established by regulated financial service providers. Such responsibilities appear to extend beyond strategic activities (*review/approval of the framework, review of operational resilience management information*) to reach operational activities (*review of Scenario testing results and of service remediation plans*). This approach diverges from the approach adopted in the *EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)* and in the *EBA Guidelines on ICT and security risk management* (EBA/GL/2019/04). In these Guidelines, the ***management Body*** and ***senior management*** of the regulated entity are assigned a broad governance role covering oversight and day-to-day management. To provide further context, the definition of Management Body adopted by the EBA Guidelines for payment institutions or electronic money institutions points to *"directors or persons responsible for the management of the payment institutions and electronic money institutions and, where relevant, persons responsible for the management of the payment services activities of the payment institutions and electronic money institutions"*.

	We encourage the central bank to afford further operational flexibility to regulated financial providers to manage the day-to-day operation of their operational resilience framework by allowing management teams of RFSPs to "own" all framework operational activities (*scenario testing, business service mapping, impact tolerance setting etc.*). Boards can retain ownership of strategic framework activities.
Identification of Critical or Important Business Services	We encourage the central bank to provide further clarity on the Criteria that RFSPs should use to designate Critical/Important Business services. We also want to highlight the need for any further central bank guidance on this topic to align with the Criticality criteria listed in: ▪ Section 4 of the *EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)* and in, ▪ Section 3.3 of the *EBA Guidelines on ICT and security risk management (EBA/GL/2019/04)*.
Impact Tolerances	We note the central bank expectation that regulated financial service providers must determine Impact Tolerances for all Critical/Important business functions (Guideline 5). RFSPs are already required to carry out business impact analysis (BIA) exercises for Critical business functions (Section 3.7 of the *EBA Guidelines on ICT and security risk management).* BIA exercises identify service recovery objectives for critical business functions that denote the size of the maximum tolerable disruption to critical ICT functions (data loss, period of unavailability etc.). We encourage the central bank to clarify whether service

	recovery objectives established through such BIA exercises align with its expectations for the Impact Tolerances outlined in Guideline 5 of CP 140.
Mapping	EMA Ireland has no comment to offer in this section of the Guidance.
ICT & Cyber Resilience	EMA Ireland has no comment to offer in this section of the Guidance.
Scenario Testing	We note the central bank expectation that *a firm should document and test its ability to remain within impact tolerances through severe but plausible scenarios* (Guideline 10). We invite the central bank to provide further guidance on: ▪ The design criteria for such test scenarios, ▪ The scope of testing of different components and of operational entities that may be involved in the delivery of a Critical/Important business function, ▪ The access to Test scenario outputs that an RFSP should receive if testing is carried out by 3rd parties, ▪ Expectations for the timeline of deployment of remediation plans to address any breach of the Impact Tolerances of Critical/Important business functions reported through scenario testing.

Respond & Adapt	
Business Continuity Management	EMA Ireland has no comment to offer in this section of the Guidance.

Incident Management	EMA Ireland has no comment to offer in this section of the Guidance.
Communication Plans	EMA Ireland has no comment to offer in this section of the Guidance.

Recover & Learn	
Lessons Learned & Continuous Improvement	EMA Ireland has no comment to offer in this section of the Guidance.

General Feedback
As noted above, we expect the adoption of the cross-industry guidance on operational resilience to lead to additional operational complexity for all regulated financial service providers. We encourage the central bank to: ▪ Adopt a proportionate approach in its supervisory assessment of alignment of regulated financial service providers of different size. ▪ Align the timeline of application of the guidance with other EU policy initiatives on operational resilience (e.g. the DORA regulation). ▪ Afford the management team of the regulated entity more flexibility in the day-to-day management of the operational resilience framework rather than placing such responsibility on the Board, ▪ Facilitate the reuse of collateral that RFSPs already generate to comply with existing EBA Guidelines (on outsourcing arrangements, on ICT and security risk management) to demonstrate readiness to apply the guidance.

Members of the EMA, as of July 2021

AAVE LIMITED
Account Technologies
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
American Express
ArcaPay Ltd
Azimo Limited
Bitpanda Payments GmbH
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Circle
Citadel Commerce UK Ltd
Contis
Corner Banca SA
Crosscard S.A.
Crypto.com
Curve
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
emerchantpay Group Ltd
ePayments Systems Limited
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
Modulr FS Europe Limited
MONAVATE
Moneyhub Financial Technology Ltd
Moorwand
MuchBetter
myPOS Europe Limited
OFX
OKTO
One Money Mail Ltd
OpenPayd
Own.Solutions
Oxygen
Park Card Services Limited
Paydoo Payments UAB
Paymentsense Limited
Payoneer
PayPal Europe Ltd
Paysafe Group
Plaid
PPRO Financial Ltd
PPS
Remitly
Revolut
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Snowy Pay Ltd.
Soldo Financial Services Ireland DAC
Square
Stripe
SumUp Limited
Syspay Ltd
Token.io
Transact Payments Limited
TransferMate Global Payments
TrueLayer Limited
Trustly Group AB
Uber BV
Vitesse PSP Ltd
Viva Payments SA
WEX Europe UK Limited
Wirex Limited
Wise
WorldFirst
WorldRemit LTD