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

José Manuel Campa
Chairman
European Banking Authority
EUROPLAZA
20 Avenue André Prothin
92927 Paris La Défense
France

14 December, 2020

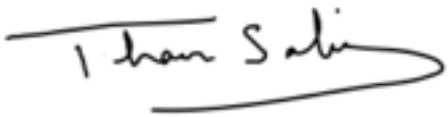
Dear José,

Re: EBA revised Draft Guidelines on the revision of the Guidelines on major incident reporting under the Payment Services Directive 2

The Electronic Money Association is the trade body for electronic money issuers and innovative payment service providers. Our members include leading payments and e-commerce businesses worldwide, representing online payments, card-based products, vouchers, and those employing mobile channels of payment. We also represent a growing number of TPPs – both PISPs and AISPs. Please find full list of our members attached to this letter.

We welcome the opportunity to respond to the EBA's consultation on revised Draft Guidelines on CDD and AML-TF risk factors, amending Guidelines JC/2017/37. A number of proposed Guidelines on the revision of the Guidelines on major incident reporting under the Payment Services Directive 2.

Kind regards



Thaer Sabri
Chief Executive Officer
Electronic Money Association

Q1: Do you agree with the change proposed in Guideline 1.4 to the absolute amount threshold of the criteria '*Transactions affected*' in the higher impact level?

A. The EMA supports the proposed change to increase the amount threshold associated with the *Higher Impact Level* of the *Transactions Affected* incident classification criterion to EUR15m.

Q2: Do you agree with the changes proposed in Guideline 1.4 to the assessment of the criteria '*Transactions affected*' and '*Payment service users affected*' in the lower impact level, including the introduction of the condition that the operational incidents must have a duration longer than one hour?

A. We support the objective stated in the Consultation Paper of reducing the number of reported operational incidents that are not material. We perceive that the changes introduced to the Lower impact level of the '*Transactions affected*' and '*Payment service users affected*' criteria will not contribute materially to the attainment of that objective. Specifically:

    1. We support the proposed increase of the absolute amount threshold of the '*Transactions affected*' criterion to EUR500k.
    2. We oppose the proposed change of the threshold triggering logic for the '*Transactions affected*' and '*Payment service users affected*' criteria into a Disjunction (OR statement) from the Conjunction (AND statement) logic that is included in the current version of the Guidelines. This change will result in increased numbers of operational incidents being reported; many of these are likely to be non-material. We propose that the current Conjunction triggering logic is retained for these criteria.
    3. We do not believe that the proposed introduction of an additional *incident duration* threshold of 1 hour will have any significant incident filtering impact. The incident response capabilities of many PSPs (using internal or 3rd party resources) exceed 1

hour; PSPs are therefore likely to breach the lower impact level of these criteria and continue to report numerous, non-material operational incidents. We propose that the *incident duration* threshold is raised to 2 hours and is focused on Critical[1] PSP functions. The new threshold should form part of an overall Conjunction triggering logic for the lower impact level of these criteria (for example for the *Payment users affected* criterion, >5000 users affected AND >10% of the PSUs AND duration of the incident >2 hours).

4. Finally, we propose that the general *Service downtime* criterion is raised to 3 hours to act as a tool for detecting incidents that do not impact Critical PSP functions.

Q3: Do you agree with the inclusion of the new criterion '*Breach of security measures*' in Guidelines 1.2, 1.3 and 1.4?

A. We support the objective stated in the Consultation Paper of focusing PSP monitoring and reporting of material security incidents. We are skeptical that the current broad definition of the new *Breach of security measures* criterion will enable the attainment of these objectives.

   The definition of the criterion in the Consultation Paper is rather generic and high-level and can result in over-reporting of incidents of breaches of security controls that impact peripheral PSP/outsourcer systems and processes (*e.g. marketing databases, business development/sales activities, internal communication systems*). We propose that the focus of the new criterion should be on breaches of security controls deployed to protect Critical PSP functions. PSPs are already required to identify such functions as detailed in the Guidelines on ICT and security risk management and in the Guidelines on outsourcing arrangements.

[1] As defined in Sections 3.3.2 and 3.3.3 of the *Guidelines on ICT and security risk management*.

Q4: Do you agree with the proposed changes to the Guidelines aimed at addressing the deficiencies in the reporting process?

A. We support the stated objectives of improving the (i) Efficiency and timeliness of the incident reporting process and (ii) Accuracy, traceability and consistency of submitted reports.

We urge the EBA to ensure that all NCAs can provide PSPs the unique incident reference code (referenced in Guideline 2.7) immediately upon submission of the Initial report to improve incident traceability.
We find the revised text of Guidelines 2.12-2.14 difficult to navigate; the text also does not align with the statement in par.24 of the Rationale Section of the Consultation paper that points to a removal of the PSP obligation to submit Intermediate reports every 3 working days. To ensure alignment of the Guidelines with that objective we propose that the opening sentence of Guideline 2.13 is revised to read " *Payment service providers* ***should submit the last intermediate report*** *when regular activities have been recovered and business is back to normal …..*".

Q5: Do you support the introduction of a standardised file for submission of incident reports from payment service providers to national competent authorities? If so, what type of structured file format would you support (e.g. "MS Excel", "xbrl", "xml") and why?

A. We support the use of a common file template and file format for the submission of incident reports to all NCAs. Our members are agnostic on the file format that is supported as long as (i) It is common and (ii) The electronic completion (and subsequent submission) of the report can be carried out with limited user friction.

We encourage the EBA to work with NCAs to facilitate a smooth migration from national incident reporting templates that are used currently to a common template/format in the run up to the application of the revised Guidelines.

Q6: Do you agree with the proposed changes to Guidelines 2.4, 2.7, 2.12, 2.14, and 2.18 that are aimed at simplifying the process of reporting major incidents under PSD2?

A. We support the changes introduced to Guidelines 2.4, 2.7 and 2.18 to streamline the incident reporting process.

We noted our concerns on the text of Guidelines 2.12-2.14 in our response to Question 4 above.

Q7: Do you agree with the proposed changes to the templates in the Annex to the Guidelines?

A. We support the proposed changes to the Incident reporting template in the Annex of the Consultation paper with the following exception:

- The introduction of Fraud as a potential root cause for a major incident[2] in Section C2 (*Route Cause Analysis and Follow up*) of the Incident Final Report. We perceive Fraud to be the likely result of an operational/security incident rather than its cause; furthermore, Fraud can be the outcome of an incident instigated using any of the other root causes already listed in Section C2.
- We also note that all other Root Causes in this Section reference operational/security control deficiencies or cybersecurity attack methodologies that can give rise to a major incident. To ensure consistency in the identification of such Root Causes we propose that the term Fraud is replaced by *Social Engineering attacks* in Section C2 of the Incident Final report template in the Annex of the Guidelines.

General Comment

We would welcome an opportunity to establish a standardized, ***2-way*** incident notification process between our members and the relevant NCAs (or the

[2] In Section C2

EBA) whereby PSPs both submit ***and receive*** timely notification of major incidents that impact the sector.

List of EMA members as of December 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
Circle
Citadel Commerce UK Ltd
Coinbase
Contis
Corner Banca SA
Crypto.com
Curve
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
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
IDT Financial Services Limited
Imagor SA
Ixaris Systems Ltd
Modulr FS Europe Limited
MONAVATE
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 Limited
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
Wirex Limited
WorldFirst
WorldRemit LTD