



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

Nisha Arora,
Director
Consumer and Retail and Policy
Financial Conduct Authority
12 Endeavour Square
London E20 1JN
UK

2 October 2020

Dear Nisha

Re: EMA response to [FCA Consultation on Guidance for firms on the fair treatment of vulnerable customers](#)

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 that provide online payments, card-based products, electronic vouchers and mobile payment instruments. Our members include leading payments and e-commerce businesses worldwide that provide online payments, card-based products, electronic vouchers and mobile payment instruments. Most members operate across the EU, most frequently on a cross-border basis. 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 sincerely

Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

EMA response to consultation

Q1: Do you have any comments on our assessment of equality and diversity considerations of our proposed Guidance?

No comment.

Q2: Do you have any feedback on the updated draft Guidance?

The updated draft Guidance is helpful for PSPs, and generally targeted at the right level. We do have a number of considerations to raise however:

- Scope: the draft Guidance applies to firms that fall within the scope of the Principles of Business (PRIN). However it is unclear whether the Guidance also applies to the offering of services that are considered by the FCA to fall outside the scope of regulation. This might include credit/lending services such as buy now pay later (BNPL) or salary advances. We would welcome clarity on this point.
- “Indirect” customers: In the context of payments, PSPs such as those providing money remittance services face challenges around understanding the extent of their duty of care towards payees they do not have a business relationship with. A PSP may be offering a payment service to the payer, with whom they have a contractual relationship. That customer may authorise a transfer of funds to a payee who meets the definition of vulnerability. The PSP must meet anti-money laundering and fraud obligations relating to their customer, which may result in delays and therefore in a negative outcome for the payee. Is it not clear what the firm’s obligations are towards the recipient in this scenario.
- Complex distribution chains: We acknowledge the Guidance’ provision that *“where firms rely on third party providers and outsourcers, they must effectively manage these providers to ensure that their customers are treated fairly”*. Under the law of agency, the obligation is on the Principal to ensure that the agent acting on their behalf complies with the necessary requirements. However we would welcome an acknowledgement or reference in the Guidance to situations where suppliers or agents may themselves be regulated entities.
- Proportionality: We welcome the Guidance’ recognition of the different firms and business models falling within the scope of the Guidance, and the application of the principle of proportionality. We propose to add an additional factor when considering the application of the Guidance para 1.25: *“Precisely what the Guidance means for individual firms will depend on the specific context of the firm, including, amongst other factors, its size, the markets it operates in, **the type(s) of products it offers,***

and the characteristics of its target market and its customers.” Some financial services products are low value, or with little consumer risk associated with them, and therefore with low impact in terms of harm to consumers. This should also be considered when taking a proportionate approach to supervision of the Guidance.

- Identification of vulnerable customers: Many EMA members, and firms that offer single-use occasional payment products are unlikely to have access to sufficient data to identify vulnerable customers. A PSP may have visibility of an e- money balance on a prepaid card or e-wallet, e-commerce or money remittance transactions without a holistic view of the customer’s financial situation or activities and will therefore find it challenging to identify vulnerabilities without asking intrusive questions the customer may not wish to answer. We welcome the clarification that *“the Guidance does not place obligations on firms to proactively identify individual vulnerable consumers through staff interactions or the use of data analytics”*. There seems however to be a contradiction with the expectation in paragraph 3.59 that *“firms use data to identify characteristics of vulnerability in individual customers so they can offer support proactively”*.
- Availability of data: Firms using data provided by credit reference agencies (“CRAs”) to assist them in categorising potentially vulnerable customers. However the [Coronavirus Data Reporting Guidance published by the Credit Reference Agencies \(CRAs\) in consultation with SCOR](#) and [FCA Guidance on Personal loans and coronavirus](#) requests firms not to report a worsening status on the customer’s credit file during any initial or further payment deferral period. As a result CRA data no longer provides an accurate picture of a customer’s financial history and firms are unable to make this judgement. Consumers who might otherwise be identified as “vulnerable” may be overlooked due to incomplete or missing CRA data.

Q3: Do you have any feedback on our cost benefit analysis?

The cost benefit analysis appears to be thorough, and relatively accurate.

Q4: Do you have feedback on what we should prioritise when monitoring firms’ treatment of vulnerable consumers?

We welcome the adoption of a proportionate approach by the FCA in the draft Guidance, and the fact that it can be applied to a wide variety of firms. When supervising firms’ treatment of vulnerable customers, this factor plays a significant role. It is important that the FCA supervisory teams acknowledge not only a firm’s size, customer base and market, but

also the type of products that it provides, and the potential for harm towards a vulnerable customer. For example, a large number of e-money products are low value, one-time use products, where the potential harm to the consumer is low, and the cost of firm-wide measures to address potential vulnerabilities in the customer base most likely higher than the value of the product itself. E-money issuers do not have permission to offer credit, and no interest is offered on e-money accounts so they do not tend to be used as investment or savings vehicles.

Similarly, PSPs that do not have access to a large pool of data, apart from the customer's transactions, or who have limited personal interaction with consumers, may experience more challenges identifying vulnerable, or potentially vulnerable customers.

Customer communications; smaller Fintech firms may face disproportionate costs applying the obligations around tailoring customer communications to the specific needs of potential vulnerable customers in their customer base. This may be particularly true when the customer base is not large to begin with.

Q5: What types of information do you envisage it would be necessary for firms to collect, to assess the effectiveness of their policies and processes in respect of vulnerable consumers?

Policies and processes will vary significantly depending on the products offered, the target market and the size of a firm. Therefore the information to be collected will also vary.

However, some data points that may be useful for firms to collect may be:

- Training data – how many staff were trained in recognition and action related to vulnerable customers, how many have undergone refresh training
- Number of accounts flagged as potential vulnerability
- Number of complaints, upheld, root cause analyses completed

If the FCA is considering introducing a new regulatory data reporting requirement in relation to vulnerable customers, we would urge the FCA to consult publicly before introducing such a requirement. This will allow the FCA to understand whether PSPs are in a position to build or amend existing systems to generate the relevant data.

Q6: Do you have any other feedback on our proposals?

EMA members raised concerns about the Financial Ombudsman's treatment of the Guidance. To avoid inconsistent Ombudsman decisions involving vulnerable customers, we

would like to call on the FCA to ensure that the FOS makes decisions on the basis of the guidance and does not apply a separate interpretation. .

List of EMA members as of October 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](#)