

Electronic Money Association  
Crescent House  
5 The Crescent  
Surbiton  
Surrey  
KT6 4BN  
United Kingdom  
[www.e-ma.org](http://www.e-ma.org)

Mr. Griffith, MP for Arundel and South Downs,

By email: [andrew.griffith.mp@parliament.uk](mailto:andrew.griffith.mp@parliament.uk)

2<sup>nd</sup> November 2023

Dear Mr. Griffith,

**Re: Authorised push payment (“APP”) fraud and the impact of the Payment Systems Regulator’s policy decisions on small payment service providers**

The EMA is the UK and 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. They also include a large number of smaller payment service providers.

These firms provide a wide range of mainstream and niche products that benefit consumers, SMEs and corporates alike. They represent a remarkable example of innovation, efficiency and consumer-centric progress in the UK, and are fundamental to the UK’s global position at the forefront of Fintech development and innovation. Recent years have seen a surge in competition in the UK market due in large part to the regulatory environment, which has driven down costs and improved the quality of services for consumer and business customers alike. Finally, the sector has been instrumental in promoting financial inclusion, providing equal opportunities for individuals from all backgrounds to access and utilize various payment methods. Overall, the payment sector in the UK acts as a catalyst for economic growth, efficiency, and financial well-being in the UK.

However, the sector is currently under significant financial pressure, not least due to upcoming regulatory changes that will have a disproportionate impact on this sector in particular.

**EMA engagement on APP Scams**

We are writing in furtherance of the Treasury Sub-committee on Financial Services' work with respect to [Scam reimbursement: pushing for a better solution](#) carried out over the course of 2022-2023. We have followed the work carried out by the Committee on this topic closely and both support and appreciate these efforts to address the problem of APP scams in the UK. We understand the magnitude of the impact that it has on individuals in the UK.

The EMA has followed and engaged in industry developments with respect to APP scams from the outset in September 2016 when Which? Submitted their super-complaint to the Payment Systems Regulator (“PSR”). We have responded to numerous PSR consultations, participated in the PSR’s APP Scams Contingent Reimbursement Model Steering Group contributing to the development of the CRM Code, and otherwise engaged with the PSR directly through conference calls and workshops with our members.

As previously indicated, this engagement has allowed us to fully appreciate and understand the magnitude of the impact that APP scams have on individuals in the UK. We also acknowledge that the PSR is required by the Financial Services and Markets Act 2023 to levy liability on PSPs for APP scams carried out over the Faster Payments system.

### **Industry concerns**

However, there remain a number of aspects of the proposed reimbursement requirement that are of great concern to our members, with a potentially significant impact on the Fintech industry in the UK.

The most concerning and potentially damaging policy proposed by the PSR is that, under their new reimbursement rules, **PSPs should be liable towards a customer for loss sustained from an APP scam to the extent of £415,000 per individual claim.**<sup>1</sup>

This proposed liability is so extensive such that one claim, which these firms have extremely limited ability to prevent, could send a small payment service provider into insolvency. A large UK retail bank could withstand a loss of £415,000; however, a smaller payment service provider likely could not. A high-value reimbursement claim is likely to put a smaller payment service provider into insolvency.

UK retail banks are required to hold large amounts of capital, which can exceed millions of pounds<sup>2</sup>; whereas, smaller payment service providers (such as electronic money institutions and payment institutions) are required, by law, to hold only between £125,000 and €350,000 initial capital. This demonstrates the different nature and risks associated with a large UK retail bank’s business compared with that of a small payment service provider.

---

<sup>1</sup> Proposed by the PSR in their recent Consultation Paper 23-6

<sup>2</sup> Pursuant to the UK Capital Requirements Regulation (575/2013)

PSPs who are members of the EMA are principally specialist payment providers who are proscribed from lending the funds of users, and therefore are restricted in the income that they generate to transaction related income streams. The impact of any increase in cost is felt much more by these PSPs (i.e. non-bank PSPs), as they do not benefit from the cross-subsidisation afforded by banks. Whilst they may be able to put in place technical and operational measures that reduce the risk that their customers might suffer from APP scams, it is much harder for them to absorb the cost of an APP scam, or the cost increase of FPS scheme fees.

As an example, if the total revenue generated by a PSP was in the region of 1% of the value of a transaction (which is generally at the high end), from which its cost of doing business must be extracted, it would have to process at least 100 equivalent size transaction to recover the loss on a single claim of fraud. Once the costs of doing business are taken into account, this is likely to increase to perhaps 1000 equivalent transactions.

### **Lack of rationale for such a high liability cap**

There is no sound basis for the PSR to propose such extensive liability. The PSR have proposed £415,000 on the basis that this is the upper limit of what the Financial Ombudsman can award to a complainant. This is not a sound basis because the Financial Ombudsman (“**FOS**”) serves a different purpose to that of the PSR’s reimbursement rules, and is not bound to decide complaints in accordance with PSR directions. The purpose of the FOS is to provide redress to customers when firms have done something really wrong or egregious, such as serious regulatory non-compliance that results in loss to the customer. The PSR reimbursement rules, on the other hand, make payment service providers the insurers of last resort for APP scams (i.e. liable in cases where they have not done anything non-compliant or otherwise wrong, just like an insurance company pays out a policy). Where the customer is receiving reimbursement for an APP scam due to no fault on the part of the firm (and the firm’s role is confined to the insurer of last resort), the extent of liability should be much lower. In the (extremely rare) cases where a customer suffers loss higher than £30,000, they can have recourse to the FOS, which has the right to award in the customers’ favour up to the £415,000.

The proposed cap of £415,000 is designed to cover 99.98% of all claims and 95% of all losses; however, 95% of APP scam claims are lower than £10,000, thus the vast majority of claims would still be reimbursed if liability was limited to £30,000.<sup>3</sup> There does not appear to be any rationale to substantiate levying such a significant liability for the sake of outlying cases, especially given the potential impact on smaller PSPs.

**For the sake of an outlying 5% of claims, we are running the risk of sinking a small payment service provider.** This would have wider ramifications. Indeed, an individual customer who fell victim to a large scam would be reimbursed; however, a small business could

---

<sup>3</sup> UK Finance Annual Fraud report (2022 data)

enter insolvency and numerous individuals would lose their jobs. In the current cost of living crisis, why would an individual customer's reimbursement take precedence over people's jobs?

Instead we support setting a liability limit of £30,000. This is the same as the liability cap for credit card fraud set down by Section 75 of the Consumer Credit Act 1974. It makes sense that the extent of reimbursement liability is consistent across all types of payment fraud.<sup>4</sup>

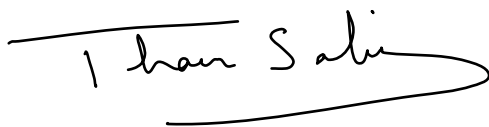
A liability cap of £30,000 ensures that a significant majority of APP fraud cases are reimbursed (i.e. 95%), whilst protecting small payment service providers from outlying cases of hundreds of thousands of pounds that would sink them.

### **Impact on the market**

It is not feasible from a competition perspective for reimbursement liability to be as extensive as currently proposed by the PSR. The result of levying such extensive liability is that start-ups and smaller PSPs will be subject to such a high liability that their ability to compete with high street banks will be reduced, and resulting in a dampening in the market. External investment in the Fintech sector may migrate towards the EU, where the liability regime for similar types of fraud will likely be much more proportionate. We would very much welcome an assessment of the impact of these proposals on competition in the sector and on PSP businesses before adoption.

We would be grateful if you would consider taking forward an action such as inviting the PSR to a committee meeting to address the impact of their proposals on the UK fintech industry (in particular start-ups and small PSPs) and on competition in the UK (as they are the competition regulator).

Yours sincerely



Dr Thaer Sabri  
Chief Executive Officer  
Electronic Money Association

---

<sup>4</sup> [Other liability caps cited by the PSR in CP23-6 such as the FSCS and FOS caps are scaled to other types of risks.](#)

**EMA members as of November 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](#)  
[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](#)  
[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](#)