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

Access to basic retail financial services inquiry
Treasury Committee
House of Commons
London
SW1A 0AA

5 April 2017

Dear Sirs

Re: EMA comments to the inquiry on access to basic retail financial services

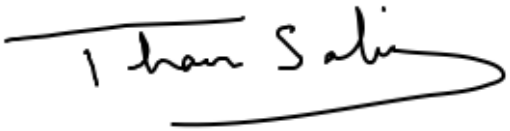
The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide that provide online payments, card-based products, electronic vouchers and mobile payment instruments. Most members operate across the EU, most frequently on a cross-border basis. A list of current EMA members is provided at the end of this document.

Please find below our comments to the Treasury Committee inquiry into access to basic retail financial services in relation to de-risking. Please feel free to contact us should you have any questions or require further information.

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

Yours faithfully

Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association



De-risking

The issue of de-risking impacts firms with electronic money products as well as those offering money remittance services. There are a number of categories of e-money providers who *are* particularly affected:

- Providers of new or innovative payment services,
- Providers that are part of groups that have a money remittance business (a number of MSBs and payment service providers ("PSPs") are moving towards obtaining e-money licences),
- EMIs offering gambling services, and
- EMIs offering services for the underbanked (e.g. immigrants and foreign students).

Whilst EMA members have existing banking arrangements, some are currently experiencing increasingly onerous requests for information from their banks, and more stringent ongoing assessments, sometimes followed by a termination of services.

Banks appear to regard themselves as responsible for any potential compliance failings by their regulated clients, acting in effect as a pseudo regulator. As a result, they appear to be setting a high threshold for revenue generation by PSP clients, that justifies the burden of managing this perceived risk.

We believe this misconception is at the heart of the problem, and would benefit from a clarification by the regulator that failings by a regulated firm, particularly where this firm is based in the same jurisdiction as the bank, would not result in enforcement action against the bank. In other words, there should be a clear boundary in the regulatory responsibility of the regulated credit institution, and compliance failings by a regulated client institution.

This could by itself greatly increase banks' appetitive to provide banking services to smaller payment service providers.

Scale

Banks that have been mentioned by EMA members in the de-risking context include:

- RBS, UK
- HSBC in the UK and France,
- BNP Paribas,
- Danske Bank,
- Banco Intesa,
- Bank of Ireland,
- Santander,
- Metro Bank,
- Lloyds,
- Nordea Finland,
- ABM AMRO Netherlands,
- BBVA Spain,

- Banca Monte dei Paschi.
- BRD Bank in Romania
- ING Bank; Czech Republic
- The Central Bank of the Czech Republic has stipulated that they will not accept Gibraltar as a jurisdiction for the holding of safeguarded funds and are insisting that funds for programmes operating in their jurisdiction are required to be held with UK banking institutions.

Relevant issues raised in the EMA's response to the HMT consultation on PSD2

We responded to the HMT consultation on PSD2 on 16 March 2017 with the following comments that impact access to bank accounts:

Second Payment Services Directive ("PSD2")

Article 36 of PSD2 introduces an obligation on member states to ensure that there is access as an outcome. In other words, in addition to introducing a requirement for non-discrimination, and for duly motivated decision, member states are required to ensure that access as an outcome is achieved.

We would therefore suggest providing explicitly for the PSR to review access to bank accounts on a periodic basis, and to review the reports from credit institutions ("CI") to establish whether the objective of access is being achieved in practice.

Furthermore, it would be helpful if the review process that the FCA or PSR exercise in relation to reports of refused applications is published, and that actions that the competent authorities ("CAs") undertake as a consequence are transparent. It would, for example, be helpful to know whether affected firms may be able to make submissions to the regulator where they feel the process has not been executed reasonably or fairly.

Applications

PSPs invest significant time and resources into verifying identity and submitting information to banks when seeking to open a bank account. The initial PSP request to open a bank account should therefore be considered the application.

Any further information required from the PSP should be requested as soon as the process commences, and where a single factor is deemed sufficient for refusal, this should be communicated to the PSP. Prompt notification from a CI informing a PSP of the outcome would enable the PSP to seek alternative solutions, and minimise wasted effort. Protracted processes and delays in making a decision could provide CIs with an opportunity to decline PSPs without having to report an actual decision.

CIs should furthermore be required to notify the PSP as well as the CA of a refusal and provide duly motivated reasons referring back to their formalised criteria for acceptance.

Success of an application is also dependent on the professional assessment of the application, the knowledge of assessor, and their understanding of the sector. Addressing competence in this area is also key.

Risk assessment and AML obligations

It would furthermore be useful to understand how the assessment of high risk is determined, providing for how mitigating measures that may have been applied have been taken into consideration. This is particularly significant where money laundering risk is a factor in decision making, and therefore a risk-based approach that considers both risk and mitigating measures should be applied.

This could reduce erroneous risk assessments, and prevent a risk assessment being influenced by a single factor.

In EMA members' experience, CIs (banks) seek to construct an internal business case for the new customer, based on the banking services that the PSP is seeking from them (e.g. types of account and services, FX requirements, deposit and borrowing capabilities). CIs then assess the financial returns they foresee against the compliance risk profile posed by the PSP.

Generally, non-bank PSPs are regarded as higher risk, notwithstanding that they are regulated entities directly by the CA. A rationale for such an assessment should be expected in any report received by the CA. Particularly in relation to MSBs, it seems inappropriate that the CI's CDD processes should include a review of their compliance policies. This suggests that the regulator's supervision is inadequate, and the CI is in a better position to assess compliance and that they are not only responsible for their own compliance, but ALSO that of their customers. Regulators must take responsibility for the firms that they regulate, and banks should be able to assume a properly authorised institution has in place adequate AML policies and practices. It is not the role of the CI to supervise or guide on AML obligations.

CIs do not share the internal benchmarks for financial returns that they seek from non-bank PSPs, nor the manner in which they assess any compliance risk posed by the PSP. Publication of such criteria, or making them available to bona fide applicants, would assist PSPs in identifying suitable CI service providers.

It would additionally be helpful if CIs could provide AML policies and procedures that they regard as the norm, so that these could be used as a reference for PSP's making applications. Ideally, these should be commonly accepted standards, such as those of the JMLSG, setting out areas of departure where necessary.

It would be helpful to encourage CIs to work with PSPs to better identify suspicious transactions, for example, in relation to information accompanying funds transfer requirements, typologies or market intelligence.

The delivery of payment services by PSPs, both domestically and internationally, requires a number of functionalities to be present. These are enabled by access to the following types of bank account:

- Pay-in accounts to receive funds from clients, which may also be segregated, and compliant with safeguarding requirements under the EMR or PSR.
- Operating accounts to manage PSP's working capital and to make day-to-day transactions without co-mingling PSP's funds with their clients' funds.
- Stand-alone safeguarding accounts for meeting safeguarding obligations.
- Other accounts such as those from which payments can be settled with payment schemes.

The meaning of "*sufficiently extensive*" access and enabling of "*unhindered*" provision of payment services under Article 36 of PSD2 would benefit from clarification by way of regulatory guidance. The objective is to access payment accounts for the purposes of making payment transactions on behalf of clients, safeguarding funds and the administering of operational accounts.

List of EMA members as of April 2017:

24 Money
Advanced Payment Solutions Ltd
Airbnb Inc
Allegro Group
American Express
Azimo Limited
Bitstamp
Blackhawk Network Ltd
Boku Inc
Citadel Commerce UK Ltd
Clydesdale Bank
Coinbase
Corner Banca SA
eBay Europe Sarl
Euronet Worldwide Inc
Facebook Payments International Ltd
FaceKart
First Rate Exchange Services
Flex-e-card
Flywire
GoCardless Ltd
Google Payment Ltd
iCheque Network Limited
IDT Financial Services Limited
Imagor SA
Ixaris Systems Ltd
Kalixa Pay Ltd
MarqMillions
Merpay Ltd.
One Money Mail Ltd
Optal
Park Card Services Limited
Payfriendz Ltd
Payoneer
PayPal Europe Ltd
PayPoint Plc
Paysafe Group
PPRO Financial Ltd
PrePay Solutions
R. Raphael & Sons plc
Remitly
SafeCharge UK Limited
Securiclick Limited
SEQR
Skrill Limited
Stripe
Syspay Ltd
Transact Payments Limited
TransferWise Ltd
Valitor
Wave Crest Holdings Ltd
Wirecard AG
Worldpay UK Limited