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

Financial Action Task Force
2 Rue Andre Pascale
75775 Paris CEDEX 16
France

23 April 2021

To whom it may concern,

EMA submission to FAFT Request for input on mitigating the unintended consequences of FATF Standards

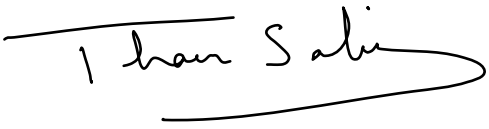
Thank you for the opportunity to provide input to the FATF's project on mitigating the unintended consequences of the FATF standards, and in particular the impact on the de-risking by banks of electronic money institutions (EMIs) and Payment institutions (PIs).

The Electronic Money Association is the trade body for electronic money issuers and innovative payment service providers ("**PSPs**"), and our members include leading payments and ecommerce businesses worldwide, representing online payments, card-based products, vouchers, and those employing mobile channels of payment. A list of our members is

The EMA has provided various submissions on the topic of de-risking to FATF in the past, and more recently to the European Banking Authority. We consider that a number of statements in the FATF Guidance on a Risk-Based Approach for MVTS Providers could be contributing to recent de-risking practices. Our specific comments are set out in the Appendix to this letter.

Please find below a summary of the EMA findings so far, as well as proposed regulatory solutions.

Yours sincerely



Thaer Sabri
Chief Executive Officer

Electronic Money Association

Electronic Money Association Member Experience of De-Risking

Geography:

EMA members have reported de-risking experiences by Financial Institutions authorised in the following member states: Germany, Sweden, Poland, Bulgaria, Lithuania, Estonia, Latvia, Malta, Italy, Australia, and the UK.

In the last 3-5 years, several EMA members who responded to recent requests for input have been de-risked or refused an account by 5-10 institutions in the EEA. Several members had been de-risked by institutions with whom they had been banking for 8-10 years with 1-2 months' notice. The firms in question had varying risk profiles and were not only small startups, but also large well-established firms with a considerable customer base.

In 2015 the EMA conducted a similar survey of members, and found that at least 15% of the EMA membership reported experiencing difficulties related to banking facilities in the previous 12 months, including large multi-national businesses who would not be expected to experience banking related difficulties because of longstanding and group wide banking relationships.

Type of account(s):

As with any business, EMIs will require banking services in order to operate. In addition to general banking services, EMIs will specifically require bank accounts in which they can safeguard customer funds received in relation to the issuance of e-money.

EMIs will therefore likely require at least two types of accounts:

1. Business bank accounts / services to manage their daily payments, e.g. salaries, rents, etc. without co-mingling the EMI's funds with their customers' funds. These can also be used to make payments in the local currency.

2. Safeguarding bank accounts –EMIs have a regulatory obligation, under the Electronic Money Regulations 2011, to segregate customer funds received in exchange for e-money issued, such that if there is an insolvency event, the e-money issued is protected from other creditors' claims and can be repaid to customers. Such funds must be held in designated and segregated bank accounts held by the EMI in EEA credit institutions. In accordance with regulatory requirements, the EMI will own these safeguarded funds, since the customers have received, and own, the e-money issued in exchange for those funds. This arrangement is significantly different from money transfer businesses, which do not own the funds associated with the transactions they process. From a bank's perspective, the EMI's safeguarded funds are the funds of its customer, the EMI (i.e. not the bank's customer's customers' money).

And possibly in addition:

3. Pay-in accounts to receive funds from clients, which may also be segregated, and compliant with safeguarding requirements under the EMRs or PSRs.

4. Other accounts such as those from which payments can be settled with payment schemes.

5. Local business bank accounts to allow access to national payment systems. EMIs and PIs are in most cases not permitted to become direct members of national payment systems, so rely on an account with a local bank in order to use the local payment system.

EMA members have had a variety of bank accounts closed or denied access to:

- Pay-in accounts to receive funds from clients
- Operating accounts to manage PSP's working capital and to make day-to-day transactions
- Stand-alone safeguarding accounts for meeting safeguarding obligations.
- Withdrawal of access to UK payment systems through banks
- Correspondent bank accounts in order to be able to settle SWIFT transactions

Impact

De-risking does not impact electronic money issuers to the same extent as for example firms offering money remittance services. However, a number of common theses have been observed:

- New market entrants: firms that are in the process of applying for an e-money or payment institutions license have experienced difficulties, sometimes having to seek banking services from another EU member state
- Firms that are part of a group with money remittance businesses have similarly experienced problems
- Electronic Money Institutions ("EMI") servicing merchants in the gambling industry, and
- EMIs offering services for the underbanked (e.g. immigrants or foreign students) are similarly vulnerable.

The time spent and the associated cost to secure and switch to new bank accounts can have a significant impact on the business: CFOs, Finance and Compliance departments and banking relationship teams have to invest a significant amount of time constantly secure new banking relationships (EMA members operating globally commented that this issue is especially acute in the EU market). Once the new account has been sourced, the cost/time required for onboarding, integration and implementation can be significant, depending on the service provided (for example offering indirect access to payment systems). These teams would otherwise be in a position to advance products and processes to improve the services offered to customers.

PSPs negotiate commercial terms when they enter into business relationships with other financial institutions: When a business relationship is withdrawn, PSPs are under time pressure to secure a new contract to avoid any disruptions for customers. In addition, the number of Financial institutions offering the currencies, links into payment systems and level

of automation needed is limited and PSPs have to therefore often accept more costly arrangements.

To mitigate the risk of being "de-banked" and no longer being able to meet regulatory obligations such as to safeguard client funds and to service customers, PSPs engage with a variety of banking partners. With an ever diminishing number of banks willing to onboard PSPs, and an increase in the number of PSPs seeking banking services, the cost has increased, and spreading the risk across multiple banks becomes almost impossible, especially for smaller market participants.

In this context it is important to note that the de-banking process can be swift (1-2 months) with little communication or formal notice whereby securing alternative banking relationships may take up to one year. Many examples were provided of firms who were given 1-2 months' notice to find an alternative solution, even during the peak of the COVID 19 crisis.

Some firms have had to consider closing the e-money segment of their business due to difficulties obtaining an account.

PSPs have to resort to using accounts offered by other PSPs instead of using bank accounts. PSPs' preference (for business continuity reasons as well as other risk management purposes) is to have several bank accounts in use in order to provide back-up in case one banking partner closes an account, but this is often not possible, and increasingly difficult to secure. This reduced choice leads to reduced choice for consumers, as non-banks face increasing challenges in this area.

In any case, securing banking relationships and keeping those business relationships are vital for PSPs to continue to operate.

Bank process and rationale for de-risking/refusing to open an account

The main argument for terminating an existing business relationship reported by the EMA's membership is the bank's risk appetite: Financial institutions perceive that the Money laundering risk associated with PSPs is outside their risk appetite as they are unable to ensure they meet their ML obligations, so they no longer wished to service the sector.

Whilst at some certain product types and/or customer segments may pose a higher ML risk – this is not the case across the whole non-bank PSP sector, and many EMA members' product offerings and customer segments are medium or low risk.

It is questionable whether financial institutions that previously serviced the PSP sector have the right to exclude or de-risk a whole sector, regardless of the risk posed by individual institutions. These strategic decisions appear to be taken by senior management with limited consideration of the individual applicant's ML risk profile or controls; instead the credit institution refuses to service the sector as a whole.

Examples have been given of banks in Italy and in Denmark limiting their service provision only to customers within their own member state.

In several instances, an existing business relationship was terminated in writing but no explanation was given.

When trying to open new bank accounts, the decision not to onboard a particular EMI was explained by a breach of the bank's policy (no EMIs, no VASPs, no EMIs servicing VASPs, etc.). In some instances an application would not progress and it would become apparent that the bank would not onboard a PSP. In other cases firms would get through a lengthy CDD process only to be denied at risk committees or similar without any detailed reasons.

The process of terminating an existing business relationship varies between banks. It is not clear to applicant PSPs what the decision- making process is or which committees may be involved in such decisions. The appeals process is likewise often opaque, with no indication whether any formal mechanisms exist at all. When EMA members appealed against banks' decisions there were several instances where they were refused the opportunity to address an internal committee (or similar) or were told that their request had been denied or that it was impossible to reverse the decision.

In other cases, where the bank was challenged citing PSD2 Article 36 (or the equivalent national provision), the bank reversed the decision. This indicates that PSD2 Article 36 has not been effectively implemented across the EEA.

Potential regulatory solutions

Implementation of PSD2 Article 36 across the EEA

In the EU, the revised Payment Services Directive 2015/2366 (PSD2) introduced a new Article 36, which obliges national competent authorities to ensure payment service providers obtain access to bank accounts with credit institutions (CIs). In addition to non-discrimination, objectivity, proportionality and a duly motivated decision by the CI, member states are now required to ensure access is achieved as an outcome.

PSD2 Article 36 offers a unique opportunity to monitor and track the extend of the problem of de-risking, as it allows NCAs to collect data in relation to declined bank accounts, and - if published - could assist industry in tracking the extent of the problem. Publication of more granular detail would also assist PSPs in identifying groups or individual CIs that are engaging with PSPs and offering banking services, thus saving resources on the side of both applicant and CI.

However the EMA's correspondence with NCAs regarding the implementation of PSD2 Article 36 across the EEA has found that there are very few Member States that have:

- Any formal mechanism in place for CIs to report to the NCA under this Article,
- Any guidance for CIs in relation to their obligations under this Article, for example at what stage a refusal to onboard must be notified to the NCA, what mechanism they should use to notify the NCA, or in what circumstances the closure of an account must be notified to the NCA.
- any formal mechanism for PIs or EMIs to submit a complaint about being de-risked, or a refusal to onboard

For example, we received responses from NCAs claiming they had received no notifications under this Article, when EMA members had either been de-risked or refused an account by a CI authorized in the same Member State, indicating that the PSD2 Article

36 reporting obligation is not properly enforced – or understood - in several EEA Member States.

As well as the above suggestions in relation to collecting and publishing data, the EMA also propose the following:

1. CIs do not currently disclose the internal benchmarks for financial returns that they apply to non-bank PSPs, nor the manner in which they assess any compliance risks posed by the PSPs. Publication of such criteria would be helpful in both understanding the requirements expected by CIs and in making the application of the process more transparent.
2. It would be helpful if the review process that the regulator exercises in relation to reports of refused applications is published, and actions that the national competent authority undertake as a consequence are transparent.
3. It would of course be helpful if affected firms were able to make submissions to the regulator where they feel the process has not been executed reasonably or fairly, or where little rationale has been provided for refusing to grant banking facilities.
4. Banks' conservative attitude and defensive posture in relation to other PSPs is a result of the perceived compliance cost of monitoring these accounts weighed against the commercial value of the individual relationship. Regulators could provide banks with 'safe harbour letters' stating that, provided appropriate risk based due diligence and ongoing monitoring is implemented, they would not be held responsible for the AML failings of their regulated PSP clients.
5. A similar right to that provided under PSD2 could be introduced, and where a bank account is refused, the regulator could nominate a credit institution to offer such services; alternatively the regulator could take a view on specific refusals and compel the relevant institution to open an account, if it felt that the refusal was unreasonable.
6. The Central Bank could consider opening accounts for such institutions at the Bank, enabling a minimum level of service to be offered; a model that is effective in a couple of EU member states;

Unintended consequences of FATF Guidance:

In 2015 in the EMA responded to a FATF CP on draft Guidance for a Risk-Based Approach for MVTS. The Guidance includes a section directed at banks taking on MVTS as customers, and at the supervisors of those banks. The EMA response raised concerns regarding the wording and related supervisory expectations set out in this section, and suggested that banks should not be involved in assessing the CDD systems of MVTS operators beyond establishing their existence, as this would establish another layer of supervision as well as more de-risking of entities in the MVTS sectors. The comments and the final outcome are set out in the appendix to this note. Essentially, the relevant paragraphs did not substantively change, so the EMA proposes to incorporate these comments into the EMA submission to the FATF.

Annex 1:

Appendix A: Excerpt from EMA response to FATF 2015 consultation on draft Guidance for a Risk-based Approach for Money Value or Transfer Services[1]

The table below sets out the concerns raised by the EMA regarding the wording and supervisory expectations that would likely lead to more de-risking of entities in the MVTS sectors, and whether any changes were adopted in the final version:

EMA comments on draft	EMA comments
Section 129 considers "being a new business without an established operating history" a higher risk factor to be included in the credit institution's analysis.	This automatically creates a barrier for startups and new entrants, as access to a bank account is one of the core requirements for the establishment of a business. This also reduces competition in the market.
Section 132 Section 132 requests banks, when they identify a higher AML/CFT risk, to "*review the AML/CFT (group-wide) programmes of the MVTS provider, their internal or external audit and other expert's reports, review the list of agents and their monitoring, management and screening practices. A visit to the place of business and/or informative statements sent to third parties to verify the alignment with operating history, where appropriate, may prove helpful to check the existence and activities of the provider. (...) additional steps or EDD may be necessary.*"	Please note that a large proportion of MVTS will be considered higher risk from a banks' perspective. Applying the requirements set out in this paragraph to the onboarding process involves considerable resource on the part of the bank. This cost is in many cases considered to be higher than the commercial benefit in taking on this category of client. Given that MVTSs are regulated directly by the competent authority, it seems inappropriate that the bank's CDD processes should include a review of the MVTS compliance policies. This suggests that the regulator's supervision is inadequate, and the bank is in a better position to assess compliance by the MVTS. This is exactly the problem that is causing the de-risking phenomenon which is currently causing disruption, as it suggests to banks 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.
Paragraph 134 states: *"Banks should have the ability to flag unusual movements of funds or transactions conducted by MVTS providers for further*	There needs to be a clear distinction between the monitoring required of MVTS transactions as a client of the bank, from those of the transactions of the customers of the MVTS. The Bank's responsibility is in relation to whether the MVTS behaves and makes transactions that are consistent with that type of business etc.

[1] Final Guidance published 2016: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf

analysis. They should also have appropriate case management systems so that such funds or transactions are scrutinised in a timely manner and a determination made as to whether they are suspicious."	It is NOT the business of the bank to consider whether a particular transaction undertaken by a client of the MVTS is suspicious. This would be untenable, and would place the bank in a position where they could not fulfil such responsibilities. They would neither have necessary access to client information, nor be in a position to assess the merits of transactions. This is again the kind of obligation that would result in banks concluding that they cannot fulfil their AML obligations in relation to MVTS and lead to the termination of such relationships.
Paragraph 141 states: "*Supervisors could encourage banks to engage with the MVTS sector on the measures that the sector could take immediately and in the longer term to meet the banks' risk standards which would enable a continuation or start of the business relationship*."	It is not the role of the banks to supervise or guide MVTS on their AML obligations. They are unlikely to understand the sector as well as the MVTS providers themselves, and the supervisory obligations are distinct. The MVTS is responsible to, and subject to the oversight of the regulator. It is required to set up its own risk management policies and not have these determined by a business supplier – in this case its partner bank. It is no more appropriate for a Bank to set the tome of risk management practices of the MVTS provider than it is of any financial institution to another. The main implication is that the competent authority is outsourcing supervision to the banks; an inappropriate and unworkable obligation. The EMA strongly objects to this wording.
The same issues arise at paragraph 160 which states: "*Banks are not expected to know the clients of the MVTS provider, but to assess the policies and procedures in place by the MVTS providers to comply with AML/CFT requirements."*	This statement appears to have been removed. The implication is that banks should take a view and decide whether the policies and procedures of MVTS businesses are adequate. This additional layer of supervision is neither welcome by banks nor by MVTS providers. Where does it stop? Should banks review every new iteration of the policies, and if so, should they do this when new legislation is issued? This is an inappropriate and disproportionate requirement.

Annex 2: List of EMA members as of April 2021

AAVE LIMITED
Account Technologies
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
American Express
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
MuchBetter
myPOS Europe Limited
OFX
OKTO
One Money Mail Ltd
OpenPayd
Optal
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
TransferWise Ltd
TrueLayer Limited
Trustly Group AB
Uber BV
Vitesse PSP Ltd
Viva Payments SA
WEX Europe UK Limited
Wirex Limited
WorldFirst
WorldRemit LTD