**Electronic Money Association**
Crescent House
5 The Crescent
Surbiton, Surrey
KT6 4BN
United Kingdom
Telephone: +44 (0) 20 8399 2066
www.e-ma.org

FATF.Publicconsultation@fatf-gafi.org

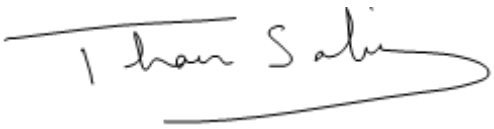
18 April 2025

Dear Madam/Sir,

**Re: Response of the EMA to the second consultation on proposed revisions to R.16/INR.16**

The EMA is a UK and EU-based trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide, providing online payments, card-based products, electronic vouchers, virtual assets and mobile payment instruments. A list of current EMA members can be seen on our website: https://e-ma.org/our-members.

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



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

## EMA response

**Para. 6 of INR.16 (paras 47, 55 and 56 of consultation): Definition of the payment chain**

The EMA strongly supports the proposal that the payment chain should be defined as beginning with the instruction from the customer.

However, we would like to draw the FATF's attention to issues arising from the proposed end of the payment chain. Under the current proposal, the payment chain is defined as ending at the bank making funds available to the final beneficiary (Bank E – please see the diagram below). This is correct if – and only if – the beneficiary does not have a business relationship with a receiving MVTS, i.e., where Customer X instructs MVTS F to transfer funds to Customer Y at Bank E, and MVTS F merely uses MVTS G as its correspondent. If Customer Y does have a business relationship with MVTS G that entitles Customer Y to receive funds from MVTS G and settle those funds in a method and to a beneficiary of their choosing, then the payment chain ought to end at MVTS G.

The reasons for this are three-fold:

1) The account of Customer Y at MVTS G may contain funds from different originators and may be used for settlement to a number of third parties unrelated to these originators. This means that funds flowing through Bank D to Bank E or Bank E2 would not be capable of being associated with individual transfers, such as the transfer from Customer X to Customer Y, making the submission of originator information with these transfers if not impossible then at least inaccurate. Instead, transfers from MVTS G to Customer Y/Y2 via Banks D and E/E2 should be regarded as transfers in which MVTS G is the originator.

   Example (please see the diagram below):

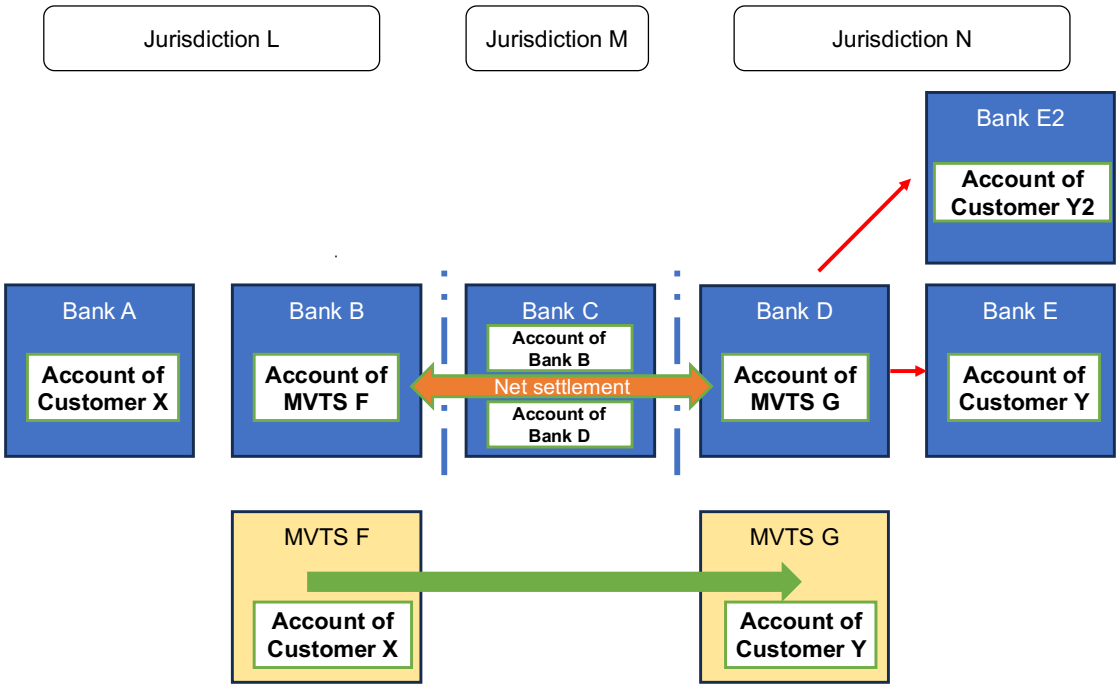
   - Customer X instructs MVTS F to transfer funds from its account with MVTS F to Customer Y at MVTS G. This is a cross-border transfer.
   - Customer Y could be a private individual or a merchant who uses their account with MVTS G to receive transfers from their customers, one of which is Customer X. This means that the funds received into Customer Y's account with MVTS G may be mixed with funds already in the account, including from other sources.
   - Customer Y then uses the funds in its account with MVTS G for a number of purposes, including making a transfer to themselves into their account held with Bank E and to one of their suppliers (Customer Y2) at another bank (Bank E2). This is a domestic transfer.
   - These settlement transfers are not transactionally linked to the transfer from Customer X to Customer Y, as they are made from a mixed fund.

2) Where Customer Y is a customer of MVTS G, MVTS G is the relevant financial institution of the beneficiary subject to full AML/CTF obligations, i.e., the financial institution that monitors, records and reports any suspicions about the transfer between Customer X and Customer Y. To require Bank D and E/E2 to also monitor the same transfer would duplicate the relevant legal obligations and disadvantage non-bank vs. bank transfers, as the latter would not be subject to duplicate

monitoring by third-party obliged entities. It should also be recognised that knowledge of transfers conducted through their direct competitors will be of competitive value to banks.

3) To require information on the originator (Customer X) to travel with the settlement transfer via Banks D and E/E2 would mean changing Bank D's status from that of the originator's safeguarding bank (the bank of MVTS G) to an intermediary for travel rule purposes. The requirements associated with this change in status would lead to increased compliance obligations, increased perceived risks and increased costs at Bank D, with the likely result of the further de-risking of recipient MVTSs such as MVTS G. De-risking in the context of safeguarding accounts for non-bank financial institutions is already an acknowledged problem that negatively impacts risk-driven diversification in safeguarding accounts and therefore increases contagion risks stemming from bank failure.

EMA-amended diagram of the payment chain




Payment chain (originator = Customer X; beneficiary = Customer Y)

Settlement step (originator = MVTS G; beneficiary = Customer Y or Customer Y2)

**Footnotes 48 and 49 of INR.16 (paras 49-51 of consultation) on account number**

Text of footnote: "In cases where the funds are drawn from a financial institution other than the ordering financial institution, the account number and the name of financial institution from where the funds are drawn should be included."

The EMA understands that the situation or typology aimed at by these footnotes is that described in paras 49 to 51 of the consultation. We think it would be useful, however, to include this limitation in scope either in the text of INR.16 itself or in accompanying guidance, as otherwise the footnotes could be interpreted as being of wider than the intended scope, counteracting the stated beginning of the payment chain by seemingly requiring the inclusion of information about the funding step with a non-bank financial institution transfer.

As a minimum, footnotes 48 and 49 should be amended to read:

> "In cases where the funds are drawn from a financial institution other than the ordering financial institution ***and the customer does not hold an account with the ordering financial institution and does not fund the transfer by either card or cash payment***, the account number and the name of financial institution from where the funds are drawn should be included."

**Paras 15-16 of INR. 16 (paras 23-27 of consultation): Goods and services exemption**

The EMA fully supports the changes made by the FATF following the first consultation. The card exemption for purchases of goods and services has been instrumental in ensuring the proportionality of the travel rule, enabling growth in international e-commerce while focusing AML/CTF efforts on areas of higher risk; its retention is welcomed.

However, we think that there are good reasons to now consider widening the scope of the exemption to other forms of payment. The payments landscape has changed significantly since this exemption was first introduced, with non-card-based electronic money and cryptoasset payments (particularly electronic money tokens) now competing directly with card payments in the e-commerce space.

Where functionality and risks, including that of fraud, are equal to those of cards, there is no longer a compelling reason not to include other payment instruments in the scope of the goods and services exemption, particularly given the transformative social effects of the opportunities provided by digital platforms, which are commonly taken up by individuals hitherto excluded from e-commerce.

Extending the scope of the exemption is also supported by the fact that the amended proposals require more beneficiary information to be submitted (including BIC/LEI), which may not be available to consumers when making a purchase online. Where consumers submit inaccurate information, this is of little use to law enforcement and represents a prohibitive cost to the financial institution of the beneficiary.

We therefore suggest that, where either the originator or beneficiary financial institution can demonstrate that the transfer relates to a payment for goods and services, the exemption should also be available for non-card payments.[1]

**Paras 18-19 of INR. 16 (paras 13-22 of consultation): Cross-border cash withdrawals (credit, debit, prepaid cards)**

We would like to caution the FATF against adopting an approach whereby it is assumed that more data disseminated to more parties in the financial ecosystem globally equals less financial crime. Fraud in particular is fuelled by the wide availability of personal data, the protection of which is dependent on both the technological and legal data protection controls present in the jurisdiction of the financial institution servicing the ATM. Any risks to personal data are only partially offset by the availability of the same data to law enforcement.

We anticipate that the requirements for cross-border cash withdrawals will have a negative impact on ATM installations and the cost of access to cash through ATMs. In this respect, we ask the FATF to consider the wider geo-political context of cross-border cash withdrawals beyond financial crime considerations. Cross-border cash withdrawals present an important means of making financial resources available to vulnerable populations.

The increased costs of ATM access, as well as the privacy and consequently fraud risks inherent in the provision of further information on the cardholder (who in most cases is also the account holder funding the transfer), will impact the cost of this service and therefore the funds that will be available for use by beneficiaries. This impact should be weighed against the risks of financial crime. In this context, it is of significant concern that the FATF has not provided a comprehensive cost-benefit analysis for its proposals.

We suggest that instead of requiring the name of the cardholder to be provided as a matter of course, this information should be requested by the ATM-servicing financial institution from the acquirer within a specified timeframe only when a suspicion arises. Linking the provision of this information to a suspicion of money laundering or fraud may facilitate the reconciliation of this requirement with data protection obligations in different jurisdictions.

Such information will be available for all prepaid cards issued in the EU, as under forthcoming European AML legislation, prepaid cards that are subject to simplified due diligence may not include cash withdrawal functionality. In the UK, the information will be available for all pre-paid card above EUR 50.

[1] Verification of payee offers one way of doing this. Open banking business cases also enable the payment initiating service provider to indicate whether the payee is a business providing goods or services.

**Para. 20 of INR. 16 (paras 38-40 of consultation): Virtual IBANs**

Text of para. 20: "Financial institutions should ensure that account numbers should not be used for obscuring the identification of the country where the accounts holding the originator and beneficiary's funds are located."

The statement in paragraph 20 of INR. 16 risks being interpreted as a prohibition on vIBANs where the country code is different from the country where the account of the vIBAN user is held ('cross-border vIBANs'). It should therefore be deleted.

As the FATF is aware, cross-border vIBANs offer important use cases, enabling (a) consumers or businesses to make payments to beneficiaries residing in other jurisdictions and (b) businesses to receive payments from customers residing in other jurisdictions. This has two key benefits, the first one being lower costs for users of vIBANs on account of the use of local payment scheme rails, the second being greater convenience for customers wishing to pay merchants for goods and services.

Without the ability to obtain a cross-border vIBANs, the cost of obtaining a local account or even setting up a local presence in each jurisdiction in order to receive payments would be prohibitive for many businesses wishing to offer their goods or services cross-border. In particular, within the EU, this could restrict the freedom to provide services. For non-bank financial institutions wishing to offer their customers the means of making or accepting local payments, the need for a local presence would similarly increase costs by impacting their ability to both access and offer competitive pricing and services. Cross-border vIBANs serve an important competitive function by driving down the cost of cross-border payments and facilitating the integration of markets for goods and services across different jurisdictions. They also effectively mitigate the harms of IBAN discrimination.

When re-considering para. 20, we would like to remind the FATF that the vIBAN issuing bank has access via the servicing financial institution to the identity of the vIBAN holder and the country in which their account is held, both of which can be disclosed to law enforcement on request. The vIBAN issuing bank also has a physical presence in the country where the vIBAN is deployed and is therefore directly accessible to local law enforcement. Additionally, under forthcoming European AML legislation, vIBAN issuing banks will be required to hold information about account holders that includes their location, further enhancing the ability of law enforcement to discover the identity and country of the account holder, should they need to do so.