May 3, 2024

Via Email (FATF.Publicconsultation@fatf-gafi.org)

Financial Action Task Force
2, rue André Pascal
75775 Paris Cedex 16 France

RE: Comments of The Clearing House on the proposed revisions to R.16/INR.16

Ladies and Gentlemen:

The Clearing House Association L.L.C. ("TCH")[1] submits this comment letter to the Financial Action Task Force ("FATF") in response to the *Public Consultation on Recommendation 16 on Payment Transparency* (the "Proposal"), which includes an explanatory memorandum and proposed revisions to Recommendation 16 ("R.16"), the Interpretive Note to R.16 ("INR.16") and the related Glossary. TCH appreciates the opportunity to provide comments on the Proposal.

Introduction

The stated objectives of the Proposal are to update R.16 to account for changes in payment business models and messaging standards, to ensure that R.16 remains technology neutral and to adhere to the principle of "same activity, same risk, same rules." The Proposal also is a part of the G20 Priority Action Plan to progress work on making cross-border payments faster, cheaper, more transparent and more inclusive. We appreciate FATF's efforts and recognize the importance of R.16 to law enforcement, financial intelligence units and financial institutions. We offer comments intended to improve the Proposal and to raise considerations that merit further deliberation in FATF's wider consultation process.

As discussed further in our comments below, TCH

- Is concerned that the costs and risks of including the proposed additional information about originators and beneficiaries in qualifying payments outweigh the incremental financial crimes benefit of the information;

[1] TCH, the oldest banking trade association in the United States, is a nonpartisan organization that provides informed advocacy and thought leadership on critical payments-related issues. Its sister company, The Clearing House Payments Company L.L.C., owns and operates core payments system infrastructure in the United States, clearing and settling more than $2 trillion each day. *See* The Clearing House's web page at www.theclearinghouse.org.

- Strongly opposes the proposed requirement for beneficiary financial institutions to check the alignment of beneficiary information;
- Suggests that additional work is needed to better define the elements of ISO 20022 messages for financial crimes purposes;
- Believes that the ordering financial institution of a cross-border payment is the financial institution that is instructed by the originator to pay a foreign beneficiary (Option 1);
- Does not support the proposed change to the net settlement exemption and believes FATF's concerns would be better addressed by more consistent application of FATF's existing recommendations to all financial institutions, including money value transfer service providers; and
- Requests that the card exemption be applied to purchase transactions conducted through any payment network that has an AML/CFT risk profile similar to payment card networks.

Comments

I. *Qualifying Cross-Border Transfers – Additional Beneficiary and Originator Information*

The Proposal would modify INR.16 to require additional beneficiary information (and additional originator information) to be included in payment messages for qualifying cross-border transfers, *i.e.*, cross-border transfers above the *de minimis* threshold. We appreciate that there may be an incremental benefit of including such information from anti-money laundering and countering the financing of terrorism ("AML/CFT") and economic sanctions perspectives. We also acknowledge that some countries may already require payment messages for cross-border funds transfers to include information of the type that FATF is proposing to require. We further recognize that harmonizing R.16 with the requirements of countries that currently mandate the information would reduce the number of payments that are stopped because more information is required by an intermediary or beneficiary financial institution. However, we have concerns about requiring the additional information and believe these outweigh the potential benefits of this element of the Proposal.

As an initial matter, requiring additional beneficiary information is likely to cause friction in the funds transfer process that is inconsistent with the G20 goal of decreasing the cost and increasing the speed of cross-border funds transfers. Specifically, the ordering financial institution may face challenges in having to collect additional information on the beneficiary. It is not customary in the United States for an originator to need the address or town name or, for that matter, a government-issued identification number or, for a natural person, date and place of birth, of a beneficiary to instruct a payment to the beneficiary. Relatedly, it is not customary in the United States for a beneficiary that is a natural person to provide such information in order to receive a funds transfer, and we expect that there will be significant hesitation on the part of

natural person beneficiaries to provide such information to originators. There may also be hesitation from legal person beneficiaries to provide such information. Thus, requiring this additional information for qualifying cross-border transactions has the very real potential to slow the process of sending funds transfers that has developed in the marketplace and even impede some cross-border funds transfers altogether.

We also have reservations about whether an originator that is faced with these additional information requirements will make the necessary effort to ensure that the additional information about the beneficiary is correct. Thus, it is unclear the degree to which financial institutions would rely on the information. For this reason, we have doubts regarding the efficacy of requiring originators to provide information to ordering financial institutions that is beyond the scope of information an originator would ordinarily possess in an underlying transaction or interaction with a beneficiary.

Moreover, in jurisdictions such as the United States, in which the proposed new information about the originator and beneficiary is not generally required, financial institution systems and electronic customer interfaces may require reconfiguration to be able to collect and transmit such information. This process would require substantial time, and we expect that the expense will not be insignificant.

In addition to the operational challenges and costs of requiring additional information in qualifying cross-border transfer payment messages, the proposed change raises significant privacy and data protection concerns. As payment models have evolved and more nonbank participants have begun offering funds transfer services, we question from a financial privacy perspective whether it is safe to have these participants holding more personal financial information of originators and beneficiaries. In the United States, for example, licensed money transmitters may offer funds transfer services to originators that compete with bank funds transfer services, yet licensed money transmitters are not subject to the rigorous data security legal requirements that apply to banks. Nor are these nonbank entities subject to comprehensive federal regulatory supervision and examination pursuant to which compliance with financial privacy laws and data security requirements is monitored and evaluated. Licensed money transmitters in the United States also are not subject to federal regulatory standards that impose substantial obligations on banks to manage their use of service providers, vendors and other third parties involved in their business activities. In practice, this means that an unlicensed entity that is involved in the funds transfer process for a licensed money transmitter (*e.g.*, a technology service provider) is potentially less regulated and supervised with respect to financial privacy and data protection than its money transmitter customer.

Finally, originators themselves, most of which are wholly unregulated from a financial services perspective, would be required to possess a level of detail regarding beneficiaries that will increase financial privacy and data protection risks. We anticipate that legal entity originators that send cross-border funds transfers on a regular basis would retain the additional beneficiary information in their accounts payable systems and thereby increase the number of places where the data can be compromised. While the compromise of originator systems is a risk that exists today, the risk would increase because cyber criminals could gain access not only to the names and account numbers of beneficiaries that exist in systems today but also government-

issued identification numbers and dates and places of birth. The exposure of this information would increase the risk of identity theft for natural persons.

In sum, we are concerned that the operational, commercial, financial privacy and data protection costs and risks of the proposed change to the required information for qualifying cross-border transfer payment messages is not justified by the incremental financial crimes compliance benefit that would result from the inclusion of the additional information in such payment messages. We encourage FATF to further evaluate these and other potential costs and risks of this proposed change. Furthermore, we discourage FATF from adding any new information components to the required information elements in a payment message without serious consideration of the financial privacy and data protection implications in FATF member countries that have not enacted common data security standards and equivalent supervision of such standards for both bank and nonbank originators of funds transfers.

II. ***Requiring Beneficiary Financial Institutions to Check for Alignment of Information***

In the Proposal, FATF identifies the growth of push-payment fraud, *i.e.*, fraudulently induced credit transfers, as a serious problem that has attracted the attention of national authorities. FATF proposes to address the problem in INR.16 by requiring beneficiary financial institutions to check the alignment of beneficiary information in payment messages with the beneficiary information they already hold in the case of qualifying cross-border transfers. FATF explains that it uses the term "alignment" to provide flexibility and that it does not envision that an exact match will be expected in all cases. Rather, it believes that the term "alignment" will allow for countries and beneficiary financial institutions to employ a risk-based approach.

TCH agrees with FATF that the growth of push-payment fraud is an important problem that merits public policy discourse. However, TCH strongly opposes FATF's proposed approach because it will materially slow funds transfers and undermine the goals of the G20 related to cross-border funds transfers, be expensive and burdensome for beneficiary financial institutions to implement and radically alter the well-established and carefully balanced liability framework for funds transfers in the United States. Further, while we appreciate FATF's intention to help with the problem of push-payment fraud, we believe it is not a problem that can be solved by INR.16.

As FATF likely understands, beneficiary financial institutions do not have the ability today to check the "alignment" of beneficiary information in a payment message with their own information about the owner of the account. Such capabilities would be new and would require an evaluation of payment messages before they could be credited to the beneficiary's account. We appreciate that FATF intends to provide flexibility in its formulation of the proposed requirement so that financial institutions could take a risk-based approach to complying with the requirement. And while we agree that a risk-based approach would be necessary for a such a requirement, we are very concerned that a risk-based approach is not enough to prevent the negative impact to funds transfers that we describe below. Instead, we expect that initially or over time, whether by law or through regulatory oversight, the FATF "alignment" requirement will translate into a requirement for beneficiary financial institutions to determine that information is a match. Also, in this context, a risk-based requirement will have the result of a strict requirement – *i.e.*, a practical obligation, if not an exact legal obligation, of beneficiary

financial institutions to review every transaction for matching information. Moreover, while on the one hand it would be important that financial institutions determine for themselves to what degree beneficiary information in a payment message needs to be consistent with their own information, on the other hand, the lack of specificity would subject financial institutions to legal claims and possible regulatory criticism that their implementation of the "alignment" requirement was insufficient.

We note that even a requirement to "check" the "alignment" of the name of a beneficiary in a payment message with the financial institution's name for the account holder – a "check" that is often assumed to be simple – is not simple. There will frequently be innocuous mismatches in the beneficiary name in payment messages and a financial institution's name for the account holder. Names may mismatch due to the presence or absence of initials, middle names or suffixes. Commonly, accounts are owned by more than one person but only one is named in the payment message; similarly, it is not unusual for a legitimate business to be known by a name that is different from its legal name (*e.g.*, a DBA name).[2] And for cross-border payments in particular, the name of the beneficiary may be provided in a different language or a different character set than the name that is received by the beneficiary financial institution because the text has been transliterated. There are also differences across countries in how information is collected and used in payment messages and deposit record systems (*e.g.*, some countries may permit the use of aliases, such as email addresses or informal names rather than legal names, or abbreviations in names of natural persons; other countries may use different ordering of surname and given name for natural persons). Hence, a beneficiary financial institution may receive a payment in which the beneficiary is identified in a manner that is normal under the laws or practices in the sending country but is different than the way financial institution customers are identified in the receiving country.

The practical difficulty of "aligning" information about a beneficiary is aggravated by the vague standard proposed by FATF. It is unclear what information about the beneficiary in the possession of the beneficiary financial institution would need to be checked for "alignment" with the beneficiary information in a payment message. Moreover, if beneficiary addresses, government-issued identification numbers, dates and places of birth are all included in payment messages, the presence of this information will lead to the assumption that financial institutions should be checking for "alignment" across all these types of information. The more data that a financial institution must "align," the higher the probability that some element will not "align," especially since the beneficiary information in the payment message will rarely have been validated by the originator. We are concerned that "alignment" might also be claimed in litigation or in a regulatory context to require financial institutions to consider not only the beneficiary information in the payment message but also whether the purpose of the payment, as

[2] While there are name matching algorithms that can be used to assist with some of these issues, the algorithms are less reliable with longer, more complicated names and can only indicate the likelihood or probability that the name in a payment message matches the beneficiary financial institution's records. Use of such an algorithm would not protect beneficiary financial institutions from the kinds of legal claims and potential regulatory criticism that we discuss in our comments.

indicated by purpose codes or remittance details, "aligns" with the financial institution's information about the "usual" activity for a beneficiary.

In addition to these practical implications, the proposal to require beneficiary financial institutions to check the alignment of beneficiary information in payment messages with the beneficiary information they already hold is unacceptable because it would alter the long-established allocation of liability for erroneous or fraudulently induced funds transfers in the United States and possibly other jurisdictions. In the United States, Article 4A of the Uniform Commercial Code, as adopted by the states, sets out a carefully balanced framework that takes into account the need for financial institutions to process funds transfers efficiently through automated systems and to have clear and predictable rules for liability. Article 4A allows the beneficiary financial institution to rely on the beneficiary's account number in a payment message as the proper identification of the beneficiary when accepting a funds transfer. Only if a beneficiary financial institution has actual knowledge that a beneficiary name and account number in a payment message do not refer to the same person is it liable for crediting the payment to an account based on the account number.

FATF's proposed change to the duties of beneficiary financial institutions would prevent them from relying on the account number in a payment message and thus deprive them of a fundamental protection of Article 4A. Consequently, beneficiary financial institutions would become liable for scams against originators that beneficiary financial institutions have no knowledge of or control over. This would result in a significant change in the liability framework for funds transfers, many of which are high-value commercial payments.

Given the liability consequences of making beneficiary financial institutions responsible for identifying and adjudicating the suspiciousness of a mismatches between beneficiary information in a payment message and the financial institution's information, this element of the Proposal would massively delay payments. Beneficiary financial institutions would undertake significant financial risk with each funds transfer they credit to customer accounts. Hence, as a practical matter, a requirement to "check alignment" would be akin to sanctions screening: something that must be performed while the payment is in flight and before funds are credited to an account. As explained above, this would result in very high numbers of payments that "alert" because the "check" for "alignment" failed. These alerted payments would then require review and disposition.

It is foreseeable, given the radical shift in liability that would result from this element of the Proposal and the time-consuming and resource-intensive nature of investigations to "disposition" mismatches, that beneficiary financial institutions might simply reject many legitimate payments because the cost of resolving informational discrepancies and the potential liability for a misjudgment would be untenable. Thus, it is not difficult to see how the proposed requirement would not only undermine the speed and reliability for funds transfers generally but also inhibit progress on one of the priority actions established in the G20 Roadmap for Enhancing Cross-border Payments – fostering faster payments across borders.

Respectfully, this element of the Proposal is not appropriate for inclusion in INR.16, because the FATF recommendations are not intended to stop crime as a general matter but to prevent or otherwise counter money laundering and terrorist financing and to support compliance

with economic sanctions. We are also very concerned that the use of FATF standards would unintentionally restructure U.S. payment law. Thus, while push-payment fraud is an important issue, TCH urges FATF not to pursue this aspect of the Proposal. We suggest instead that FATF could assist with the issue of push-payment fraud by supporting better fraud-related data flows between financial institutions.[3]

III. ***Structured Information***

The Proposal would modify INR.16 to require information accompanying payments to be structured, to the extent possible, in accordance with the established standards of the system used, such as ISO 20022. TCH supports the use of structured formats where they are available. However, it is not feasible for all payment systems to adopt highly structured formats such as ISO 20022 and, thus, it is important that the limitations of older and less-structured formats be recognized in INR.16. This could be accomplished in the proposed modification by changing the phrase "such as ISO 20022" to "whether ISO 20022 or another standard."

With respect to ISO 20022 specifically, TCH believes that the implementation of the standard in payment systems will not yield the full financial crimes benefits that the industry and public authorities have expected until additional work is done to define more precisely elements of the new message and how they should be used. In particular, the new "ultimate debtor" and "ultimate creditor" elements do not have a clear purpose and will be used by different financial institutions in different ways unless a public-private consensus develops around the meaning of these terms. We encourage FATF to undertake this work in partnership with the private sector to realize the potential benefits of ISO 20022 for AML/CFT purposes.

IV. ***Payment Chain***

The Proposal considers defining the payment chain for purposes of determining the scope of R.16. FATF asserts that this is important because of the evolution in funds transfer business models and in particular the introduction of the money or value transfer service ("MVTS") providers as a new type of participant in the funds transfer ecosystem. FATF notes that MVTS providers may use payment flows in which a cross-border payment is treated as separate domestic payments and that the true originator (and we presume also the true beneficiary) may not be identified in one or more of the domestic payments involved in the end-to-end payment flow. TCH strongly agrees that this practice is inconsistent with the intent of R.16 and that FATF should clarify that domestic payments that carry out payments from an originator in one country to a beneficiary in another country as part of a larger, end-to-end cross-border payment must identify the originator and beneficiary (and their related R.16 information) of the end-to-end payment.[4]

---

[3] We note that, as part of the G20's cross-border payments initiative, the Financial Stability Board ("FSB") is exploring how data frameworks may enable or impede improvements to cross-border payments. We think that this work stream would be an appropriate place for FATF to share its concerns about push-payment fraud and to encourage the FSB to recognize the need for improved cross-border data sharing for fraud mitigation.

[4] We note that domestic payment message formats may not support the clear identification of foreign originators or beneficiaries, their financial institutions, or other related R.16 information. FATF should clarify that financial

In considering how to define where an end-to-end, cross-border payment begins for purposes of R.16, FATF has noted that an originator may instruct one financial institution (*e.g.*, the MVTS provider) to send a cross-border payment while funding the cross-border payment from another account held by another financial institution (*e.g.*, the originator's bank). Specifically, FATF calls out payment flows in which funds are pulled or pushed from an originator's account with one financial institution (the bank) to the originator's account with another financial institution (the MVTS provider) and then used to fund the originator's payment instruction to the second financial institution (the MVTS provider) to make a cross-border payment. We note this type of payment flow is not new. Legal and natural persons routinely transfer funds between their own accounts at different financial institutions ("me-to-me" transfers) for various reasons, including to fund payments. We recognize that under some MVTS flows, the originator may not hold an account with the MVTS provider and that the funding payment is credited to the MVTS provider's account with a financial institution without a correlating credit to an account or subaccount associated with the originator. This also is not new.

FATF proposes two possible approaches to defining the beginning of a payment chain for purposes of R.16 when a cross-border payment is ordered from one account and funded from another. Option 1 would consider the payment chain to begin with the financial institution that receives the originator's payment instruction for the cross-border payment (*i.e.*, the instruction to pay a beneficiary in another country), and Option 2 would consider the payment chain to begin with the financial institution from which the originator's funds are provided (*i.e.*, the financial institution that the originator instructs to send funds to another domestic account or that receives a debit instruction to allow funds to be pulled to another domestic account). Under Option 1, the financial institution that orders the cross-border payment would be the ordering financial institution. Under Option 2, the financial institution that the originator uses to fund the cross-border payment would be the ordering financial institution.

If FATF decides to define the payment chain in INR.16, it should do so using Option 1. This is the approach currently in effect in the United States.[5] It is the most reasonable approach for transactions in which an originator initiates a cross-border payment through an MVTS and funds the transaction from an account held at a bank. This is so because funds credited to an account are fungible and can be used for any purpose consistent with the nature of the account. In most instances, neither the bank nor the MVTS provider will be in a position to know that the funding transaction will fund a specific cross-border payment. The ambiguity results from the fact that many MVTS providers provide accounts that hold customer funds (*e.g.*, an e-wallet). Thus, a bank will not know whether a transaction that sends funds from an account at the bank to an MVTS provider is for the purpose of funding an account for later use or is for the purpose of initiating a specific cross-border payment. This is very significant as banks apply different controls to cross-border payments than domestic payments. Thus, if a "funding" bank is to be

institutions should not use domestic payment systems for cross-border payment flows, if the domestic message format, as specified by the payment system operator, for the system does not support clear identification of R.16 parties and information or cannot support the level of intermediation required by the payment flow. We believe this would be consistent with the current Wolfsberg Payment Transparency Standards.

[5] *See* 31 C.F.R. § 1010.410(f); *Id.* at 1010.100(ggg) ("transmittor's financial institution" is defined generally as the financial institution to which the transmittal order of the transmittor is issued).

identified and held to the responsibilities of an ordering financial institution, it would need to know this at the time the payment instruction for the funding transaction is received. Similarly, an MVTS provider may not know the purpose of a customer's funding transaction unless that transaction is contemporaneous with a request from the customer for a cross-border payment and, even then, the customer's intention will be unclear if the customer has sufficient funds in an account at the MVTS provider to cover the requested cross-border payment. Hence, Option 2 would require complex information flows between the originator and the two financial institutions. Such flows do not exist today.

There would also be potential legal implications unrelated to AML/CFT policy for "funding" banks if they were treated as the ordering financial institution for a cross-border payment that is instructed to another financial institution. There are laws in the United States, such as Regulation E (including the Remittance Transfer Rule) and Uniform Commercial Code Article 4A, that impose obligations on a bank that sends a payment for a customer. It is unclear how those laws would apply when there are effectively two banks being treated as sending a cross-border payment for an originator.

We are also concerned that defining the payment chain to start with a funding transaction under Option 2 would have significant implications for financial institutions generally as Option 2 would not be restricted to cross-border payments involving MVTS providers. All the practical implications noted above would also apply when a bank, rather than an MVTS provider, receives funds to a customer's account and the customer instructs a cross-border payment from the account. It is not feasible for banks to 'trace" the source of funds for every cross-border payment instructed from their accounts in order to determine if there is another financial institution that should be identified as the ordering financial institution. Nor is it feasible for a "funding" bank to ask its customer the purpose of every transfer sent from the customer's account to another financial institution.

Even in circumstances in which a financial institution knows that a particular funding payment pushed or pulled from another financial institution will fund a particular cross-border payment, the funding payment is legally distinct from the cross-border payment. Under U.S. funds transfer law, a funds transfer begins with the originator's instruction to the originating bank to pay or cause another bank to pay the beneficiary.[6] If the originating bank accepts this instruction, it must execute the instruction by either paying the beneficiary or instructing another bank to pay the beneficiary. A funding payment is not an instruction to pay the beneficiary of the cross-border payment. It is an instruction (or debit authorization) to pay the originator (if the payment is "me-to-me" between the originator's accounts) or to pay another financial institution. The fact that the funds will be used by the originator to make a specific cross-border payment does not make the funding payment itself part of the cross-border payment.[7]

[6] Uniform Commercial Code § 4A-104(a) (defining "funds transfer").

[7] In contrast, a cover payment is part of a cross-border payment because it enables the transfer of value between an ordering financial institution and beneficiary financial institution for a cross-border payment that the ordering financial institution has instructed to the beneficiary financial institution through a separate message flow. Hence, it is appropriate for the originator and beneficiary of the cross-border payment to be identified in a cover payment.

Last, the marginal value of defining the payment chain using Option 2 is limited – it would result only in the addition of the bank account number for the originator's funding account and the identification of the bank that holds the funding account for that subset of cross-border payments that are funded on a one-to-one basis from an account held by a different financial institution than the financial institution that the originator has instructed to send a cross-border payment. The benefit would be far outweighed by the complicated interaction between banks and other financial institutions that would be necessary to facilitate compliance with Option 2. We expect that these information flows would also increase the cost and further reduce the speed of cross-border payments, which is contrary to the G20's objective. In light of these issues, it is logical to follow Option 1 and start the payment chain at the ordering financial institution, whether it is an MVTS provider or a bank.

We suggest that a better approach to addressing FATF's payment chain concerns is first to clarify what an account-based cross-border payment is, namely an instruction by an originator to a financial institution to send a payment to a beneficiary whose account is located in another country. Second, FATF should emphasize that a financial institution must treat any payment instruction for an account-based cross-border payment that it sends to another financial institution (whether through a domestic payment system or an international messaging service) as part of the end-to-end cross-border payment and comply with R.16 requirements accordingly. Third, FATF should apply the "same activity, same risk, same rules" approach to MVTS providers that is applied to banks. This would mean requiring an MVTS provider to perform sufficient diligence on an originator so that an MVTS provider is in a position to respond to law enforcement inquiries about the originator, just as banks are expected to do.

V. ***Net Settlement Exemption***

The Proposal would revise the exemption for net settlement between financial institutions to require that, where any net settlement results from qualifying payments or value transfers carried out on behalf of customers, parties to the net settlement apply customer due diligence ("CDD") measures to their customers for such underlying transactions and comply with applicable targeted financial sanctions. This is not the right approach on net settlement.

TCH believes that it would be more useful for FATF to clarify that, although customer payments may be settled between financial institutions through net settlements that are not subject to R.16, R.16 applies to the messages that instruct the underlying customer payments (which messages are communicated in an information flow that is separate from the net settlements). Financial institutions that send and receive the underlying customer payment messages (MVTS F and MVTS G in FATF's diagram in section (f) of the Proposal) are responsible for populating and/or using information in those messages to comply with their AML/CFT and sanctions requirements as appropriate for their role as an ordering, intermediary or beneficiary financial institution. In contrast, financial institutions that are parties to a net settlement for other financial institutions' customer payments (Banks B, C, and D in the diagram) are not ordering, intermediary or beneficiary financial institutions of the customer payments. In other words, FATF should state that the payment messaging should be transmitted end-to-end from the ordering financial institution to the beneficiary financial institution even if financial institutions that are involved in the payment flow satisfy their payment obligations to each other through a net settlement transaction.

We further note that it is not necessary for FATF to modify the net settlement exemption if it seeks to use CDD as a way to ensure that net settlement will not be used to evade AML/CFT or economic sanctions requirements. Instead, FATF should require that governments apply Recommendation 10 ("R.10"), which requires financial institutions to conduct CDD, to all financial institutions, including MVTS providers, that participate in funds transfers, including person-to-person funds transfers.

VI. ***Changes to Exemption for Certain Card Payments***

INR.16 currently contains an exemption for transactions carried out using a credit, debit or prepaid card for the purchase of goods or services. The Proposal would retain this exemption with some changes. Under Option 1, bank name and location information would need to be included in the card transaction message. Under Option 2, in addition to the bank information requirement of Option 1, the exemption would not apply – and R.16 would continue to apply – when a credit, debit or prepaid card is used to make a cross-border automated teller machine ("ATM") withdrawal or purchase of cash or a cash equivalent or is used to make a domestic ATM withdrawal or purchase of cash or a cash equivalent with a value over USD/EUR 1,000. Under both options, FATF would clarify that exempt transactions must be for the purchase of goods or services *from merchants*. We support limiting this exemption to the purchase of goods or services from merchants. However, FATF should not impose the proposed new conditions or limits of Option 1 or 2.[8]

Moreover, FATF should expand the availability of the exemption so that it applies to purchase transactions conducted from a merchant through *any payment network* that has an AML/CFT risk profile similar to payment card networks. FATF states that card payments present lower risk for illicit finance transactions because payment card networks are systems in which participating cardholders and merchants are customers of financial institutions, which in turn are contractually obligated by the payment card networks to adhere to AML/CFT and sanctions compliance measures. Other payment networks that have these same attributes may be used currently or in the future to facilitate purchases of goods and services. For example, TCH operates the RTP® network, a real-time payments network that is a system in which all participants are depository institutions and subject to U.S. governmental supervision for risk-based AML/CFT and sanctions compliance programs. The RTP rules expressly require participants to have a written sanctions compliance program. RTP payments could facilitate payments to merchants for the purchase of goods or services in the future. Consistent with FATF's principle of "same activity, same risk, same rules," RTP payments used for the purchase

---

[8] In our experience, payment networks work well with law enforcement to provide requested bank information; hence, the need for Option 1 is unclear. With respect to Option 2, (1) in all ATM withdrawals, the originator and beneficiary are the same person as far as the financial institutions are aware, and consequently there is no utility to requiring the full set of information required under R.16; and (2) the AML/CFT risks associated with a purchase of cash or cash equivalents are better addressed by subjecting all sellers of cash or cash equivalents to AML/CFT obligations, including R.16 and R.10.

of goods or services from a merchant should be treated the same as card payments used for such purchases.[9] Doing so would ensure a level playing field for similarly situated networks.

* * *

If there are any questions regarding our comments, please do not hesitate to contact the undersigned at +1 (336) 769-5302 or alaina.gimbert@theclearinghouse.org.

Sincerely,

Alaina M. Gimbert
Senior Vice President & Associate General Counsel

[9] If RTP payments used for the purchase of goods or services from a merchant were treated the same as similar card payments, the concept of the "credit or debit or prepaid card number" would presumably be translated to apply to the "account number" of the originator.