The Wolfsberg Group
c/o Basel Institute on Governance
Steinenring 60 | 4051 Basel, Switzerland

10th May 2023

Ms Tara Rice
Head of Secretariat
The Committee on Payments and Markets Infrastructure
Basel
Switzerland

Dear Ms Rice/Tara,

The Wolfsberg Group (the Group) welcomes the opportunity to comment on the report issued by the Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI) on ISO 20022 harmonisation requirements for cross-border payments. The Group is an association of thirteen global banks[1], founded in 2000, which aims to develop frameworks and guidance for the management of financial crime risk and has always viewed the payments business as a key financial crime compliance risk area. This dates as far back as the Group's support of the Financial Action Task Force's Special Recommendations (specifically Special Recommendation VII on wire transfers) in its 2002 Statement on the Suppression of the Financing of Terrorism and developed further in the Group's 2007 Statement on Payment Message Standards (made jointly with the Clearing House Association). The Group then provided significant institutional support to Swift (and partnering competent authorities) in the launch and implementation of the MT202COV message and in 2017 published the Wolfsberg Group Payment Transparency Standards, which included strong advocacy for ISO 20022; this Standards document is currently in the process of being updated.

The Group believes that harmonising payment and messaging formats globally around the ISO 20022 standard offers considerable benefit to the industry in the form of more data, more structured data (making it easier to analyse), and potentially enhanced transparency (due to the differing amounts of data being able to included in different payments and messaging systems) once the format is adopted fully and to the extent that all relevant payment systems adopt it. We welcome the introduction of the format and the CPMI's thoughtful analysis of ways to improve harmonisation.

Today, the types of entities and the payment and messaging systems used by those entities to move funds are no longer as simple as when cross-border payments (outside of those made in cash) moved almost entirely through regulated banks via Swift messages. Payment activity includes more numerous and varied intermediaries with the entry of new providers and innovation has led to payment systems being used for purposes other than those for which they were originally designed. Payments may be 'fragmented' by being collected in one jurisdiction using local low value systems, aggregated according

[1] The Wolfsberg Group members are Banco Santander, Bank of America, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JPMorgan Chase, MUFG, Société Générale, Standard Chartered and UBS.

to destination jurisdiction into a single cross-border payment, and then disbursed in the receiving jurisdiction using local low value systems. This 'aggregation' process (variously described using terms such as, but not limited to, bulk, batch, bundle, and netting) means that intermediaries do not see the underlying activity or even know whether the payment represents aggregated activity. In this respect the diagram on page 4, while an accurate example of how funds can move cross border, is a simplified representation of today's flows – consideration of more complex yet common types of flows with additional payment intermediaries would be necessary to make the application of the guiding principles more comprehensive.

Our comments below are focused on the questions that deal with financial crime compliance risk.

Questions 2 & 3

- Entities initiating ISO 20022 messages or payments should be primarily responsible for the selection of the appropriate message type. Where such an entity is a customer of another financial institution (FI) or Payment Service Provider (PSP), the FI/PSP[2] should have an operational responsibility to assess whether its customer is using the appropriate message types. The choice of payment channel and message type should not have the effect of avoiding detection of information by any other entity in the payment process.
- We recommend that guidance be issued that the presence of all parties (FIs/PSPs) in the payment flow must be identified in their respective fields. This will ensure payment transparency for all parties involved in the flow of funds.

Question 5 & 7

- Consideration of enabling codes used cross-border activity to by having unique codes for a country's outlying or overseas territories, and special economic/free trade zones would be highly beneficial in identifying potential different risk characteristics in payments.
- Requirements for use of cross-border codes in situations where a payment flow is fragmented thus moving through various FIs/PSPs each of which will have limited visibility or knowledge of the underlying or nature of the payments will need to be considered carefully. Usage of the codes must be consistent, and explicit requirements should be set for fragmented and aggregated payments, and the responsibilities of any intermediaries. Requirements need to consider 'conflicting' information where an intermediary or beneficiary FI/PSP receives incoming payments without the cross border code but where its understanding is that a cross-border payment is involved. If made optional, the code may not be adopted widely.
- Requiring use of a specific code for payments in respect of "goods or services" would enhance payment transparency for all parties involved in the payment chain for this activity.
- While the use of standardised codes will assist FIs/PSPs in understanding the nature of the payment, they will not necessarily provide that FI/PSP with information about the rationale behind the payment so may not hasten the processing of payments when, for example, it is necessary to determine the nature of the payment for sanctions compliance purposes.

[2] Throughout this document the term FI/PSP is used to denote any entity engaged in payment processing whether traditional banks, money service businesses, entities commonly referred to as third party payment providers, electronic money institutions, and virtual/crypto asset service providers, among other PSP types.

Question 8 – fragmented payment flows (as set out above) pose a challenge for usage of a code since a single flow can comprise two domestic and at least one cross-border payment so codes maybe appropriate at the start and end but not in the middle of the flow. It can also be the case that the value (i.e. the payment) flows via different channels to the underlying payment information and that intermediaries may see only the 'value' part of the transaction without any of the underlying payment information. We recommend that the originating FI/PSP be responsible for applying the Category Purpose code and that the code should travel with all stages of the cross-border payment flow regardless of whether individual component payments are cross-border or not.

Question 9 – the impact and cost of reconfiguring systems to include codes and then detect their present/absence should not be underestimated. Each FI/PSP will need an internal risk appetite – absent regulatory guidance - to determine whether to accept, stop/query or reject a payment without a code, which could result in payment delays.

Question 12 – a UETR that is used consistently across all steps in the payment chain and used by all payment participants, across all payment/messaging systems may assist with transparency. This would be especially useful in the example of fragmented payments where the three payment legs (two domestic and one cross-border) each have their own references. However, if the cross-border transaction is aggregated (i.e. made up of multiple payments that are being handled in bulk/as a batch/a bundle) then it would not be possible for the cross-border transaction to allow the underlying UETR's to 'travel' with it. We note that Swift currently uses its own UETR and the presence of more than one UETR would undo any benefit of a single reference and that not all cross-border payments use Swift.

Question 16 – inclusion of information about the original payment amount as instructed by the debtor/ultimate debtor would aid certain financial crime compliance detection scenarios (e.g. those identifying round amounts or transaction amounts just under reporting thresholds).

Question 18 – the operational impact of CPMI service level code will depend on its requirements. See also our response to question 9.

Question 21

- The use of an account number or other unique reference is necessary to allow an FI or PSP to identify parties to a transfer from a sanctions and AML transaction monitoring perspective.
- A unique account number at any given FI/PSP also serves to enable 'whitelisting' processes where a party with the same/similar name to a sanctioned party has (after appropriate research) been identified as not a sanctioned party – this process helps to minimise payment delays for such persons/entities[3].
- We interpret that an 'account proxy' is some kind of unique identifier for the debtor/ultimate debtor and creditor/ultimate creditor of a payment.

[3] This 'whitelisting' process is generally performed by each FI/PSP in the payment chain given challenges in relying on other entities. Once established (and assuming no changes in the sanctions regime(s)), whitelisting benefits the parties to the payment for future transactions using the same FIs/PSPs.

- If 'account proxy' includes tokenised account details where each payment has a different randomly-generated code (designed to shield the account number), this would render monitoring for suspicious activity less effective.
- Usage of an 'account proxy' must not conflict with 'confirmation of payee' processes in place in various jurisdictions.

Questions 22 & 23

- The ability to identify the name and location of each FI/PSP party in the payment chain is necessary to ensure the performance of sanctions and AML monitoring controls.
- We agree strongly that all FI/PSPs in a payment chain should appear in the payment messages so the entities having the relationship with the debtor/creditor (or any ultimate parties) are clear. In the pre-ISO20022 environment, limitations in the length or number of fields can cause party names to be dropped.
- Elimination of unstructured text by using standardised codes (e.g. BIC, LEI, IBAN, each country's equivalent of bank routing codes, etc) means that less time and energy is spent reformatting data and more time can be spent using it.
- The Swift BIC is very commonly used for this purpose in cross-border payments today but not all entities use Swift or have/will want a Swift BIC; the introduction of a requirement for a BIC for the domestic leg of cross-border payments may conflict with usage of existing local codes (e.g. IBAN and IFSC code in India)
- We note that the final paragraph of page 17 refers to the BIC in connection with reducing false positives in sanctions screening but note that it is much more common for sanctions hits to be on a debtor or creditor than on any of the FIs/PSPs involved.

Question 25

- Inclusion of uniformly structured data for all parties involved (provided there is sufficient capacity in the payment's number of fields and field lengths) will assist the AML monitoring investigations processes in terms of understanding the nature of the flow of funds, especially if the industry can agree on standardised naming conventions that would reduce the necessity of entity resolution processes.
- This will not improve cases of aggregated payments where a single payment is used to move a bulk/batch/bundle of underlying payments and the underlying party names will not be visible to intermediaries in the normal course of business. We note that implementation of ISO message formats in Swift is gradual and that all payment market participants will need time to learn and adapt to the new formats.

Question 26 – the Group recognises the potential benefit offered by the LEI or other structured identifier for transacting entities that are legal entities. Such identifiers do not assist in cases where natural persons are the transactors.

Question 27 – as mentioned at the beginning of this submission, the Group is in the process of updating its 2017 Payment Transparency Standard and one area of focus is the use of terms such as bulk, batch or bundle to denote a single payment that represents the aggregation of multiple underlying payments (whether 'one to many' , many to one' or many to many') we have identified that these terms are in common usage but without formal definitions and that the use of 'bulked' in the background and

rationale to this requirement introduces another potential meaning for this word. We caution against using the term 'bulked' in this context and suggest that the risk you're seeking to highlight in this requirement is that of concatenated data. Please also see our response to question 25 above

Question 28 – use of consistently structured address data was something encouraged in the Group's 2017 Payment Transparency Standards. Correct usage of the message formats can also serve to improve the efficiency of sanctions screening processes (e.g. by not screening a street name against the name of a sanctioned party). Appropriate monitoring would be required to ensure that payment market participants are using the message formats correctly and not, for example, placing information in incorrect fields as this could degrade legally required sanctions screening processes.

Question 29

- Party name plus country and town name would be minimum requirements for sanctions screening but would not be sufficient for AML transaction monitoring. For example, a commonly used red flag for AML transaction monitoring is multiple (unrelated) individuals using the same address and this would not be possible if street addresses were not available.
- We note that not all address fields set out in Annex 2 have CPMI Data Model tags and recommend that these be tagged for clarity on whether they are optional or not.

Question 30

- Requirement 15's maximum field lengths (140 characters of unstructured and 9,000 for structured) are the same as Swift's ISO 20022 MX standards so the intent of this Requirement is unclear. We recommend that the 'minimum size of….remittance information' not be set to be the same as the maximum.
- The Group believes that the principles set out in its 2007 Statement on Payment Message Standards be reinforced to all market participants. Specifically the first standard which reads 'Financial Institutions should not omit, delete, or alter information in payment messages or order for the purpose of avoiding detection of that information by other financial institutions in the payment process.' As mentioned above, this statement is part of the document that is being updated but the principle remains, will be extended to all parties in the payment chain and will also consider omissions, deletions or alterations that result in the loss of information (whether deliberate or not).

Question 31 – requiring parties in a payment chain to access data sources that are separate from the information contained on the face of the payment will introduce delay in processing (especially in large payment operations that may handle hundreds of thousands of payments a day). It would be a significant operational challenge to reconcile different information sources and run them through sanctions screening processes simultaneously, and the cost of synchronising these two flows of information would be a material additional expense. In the interests of not adding to payment friction, we recommend avoiding anything that compromises or impedes the ability for straight through processing.

Question 32 – while all cross-border payments using the Swift network will use the ISO 20022 format starting in 2025 (assuming no delays in the implementation timeline), this does not mean that those payments use all the rich data features and formatting available in ISO 20022. Conversion of payment initiation channels to use ISO formatting and the reprogramming of FIs'/PSPs' customer information

The Wolfsberg Group
c/o Basel Institute on Governance
Steinenring 60 | 4051 Basel, Switzerland

systems (which are usually used to populate debtor information in payments) to use ISO formatting may not be complete by 2025 and it will likely take time for all payment market participants to be using the new formats fully and correctly.

Finally, while the report acknowledges that 'fragmentation and mixed use of messaging standards' is a major friction in cross-border payments, the necessity of real time screening for sanctions compliance may be a bigger source of friction especially when a party in the payment chain requires information that is only available from the debtor or creditor. Entities in the payment chain that are legally obliged to not process payments for the benefit of sanctioned parties must satisfy themselves that a sanctions hit is a false positive to process the payment – this usually requires asking for additional information/documentation from the debtor which causes delay (especially when an intermediary FI/PSP must ask for this as they have no direct relationship with the debtor). Overall, the desire for frictionless cross-border payments is, difficult to reconcile with the real time sanctions screening required of FIs/PSPs.

We appreciate the opportunity to submit these comments for your consideration, if you require further information or have questions about the content of this submission, please do not hesitate to contact us.

Yours sincerely

Alan Ketley
Executive Secretary
The Wolfsberg Group