SWIFT Response to the CPMI Consultative Report on Correspondent Banking

7 December 2015

SWIFT welcomes the CPMI consultative report on the current trends and potential technical measures that might alleviate some of the concerns and cost issues related to correspondent banking. We thank CPMI for the opportunity to provide comments.

SWIFT is a member-owned, cooperative society headquartered in Belgium. SWIFT is organised under Belgian law and is owned and controlled by its shareholding Users, comprising more than 3,000 financial institutions. We connect approximately 10,800 connected firms across more than 200 countries and territories. A fundamental tenet of SWIFT's governance is to continually reduce costs and eliminate risks and frictions from industry processes.

SWIFT provides banking, securities, and other regulated financial organisations, as well as corporates, with a comprehensive suite of messaging products and services. We support a range of financial functions, including payments, securities settlement, reporting, and treasury operations. SWIFT also has a proven track record of bringing the financial community together to work collaboratively, to shape market practice, define formal standards and debate issues of mutual interest.

We thank CPMI again for the opportunity to comment. Please do not hesitate to contact us should you wish to discuss our comments further.

Natasha de Terán
SWIFT | Head of Corporate Affairs
Tel: + 44 20 7762 2151
Mob: + 44 7780 483 467 www.swift.com

Recommendation on payment messages: It is recommended that the relevant stakeholders determine whether the MT 202 COV payment message is as efficient and effective as intended or whether relying only on the MT 103 and the serial processing method would better serve the needs of clients, the industry and law enforcement in light of the fee structure, technological changes and payment capabilities for processing correspondent banking payments. The Wolfsberg Group seems to be the most appropriate body to review the issue and to initiate a recommendation in this field and lead any consequential changes if required.

We fully support the Committee's efforts to ensure that messaging standards continue to serve their intended purpose, and SWIFT Standards is ready to contribute expertise to any review.

It is our understanding that the fundamental problem the Committee seeks to address with the recommendations set out in the report, is that de-risking in the correspondent banking sector is leading to the loss of vital services in less-developed or riskier markets. However, in the matter of serial MT 103 versus MT 202 COV we do not see a clear link to de-risking, nor how relying on serial MT 103 would address the problem.

The cover method for international payments can bring advantages in terms of timeliness and cost-efficiency for customers and use of the MT 202 COV effectively mitigates compliance risks. We believe the MT 202 COV has an important role to play in an international payments market that is open to increasingly strong competition from non-traditional players.

Recommendation on the use of the LEI in correspondent banking: In addition to the general promotion of LEIs for legal entities, relevant stakeholders may consider specifically promoting the use of the LEI for all banks involved in correspondent banking as a means of identification which should be provided in KYC utilities and information-sharing arrangements. In a cross-border context, this measure is ideally to be coordinated and applied simultaneously in a high number of jurisdictions. In addition, authorities and relevant stakeholders (e.g. the Wolfsberg Group) may consider promoting BIC to LEI mapping facilities which allow for an easy mapping of routing information available in the payment message to the relevant LEI.

LEI is an ideal reference for KYC information because it can clearly and unambiguously identify legal entities, and is an open standard that can be used without licensing implications. Other identification schemes such as BIC, which is the party identifier currently used in SWIFT's KYC product, do not map with total precision to legal entities because in a few instances entities may have more than one BIC, whilst in a few others, a BIC can be used for transactions relating to multiple entities within the same group

Currently, all the KYC utilities have adopted their own identifiers in order to distinguish between entities. Whilst this enables the unambiguous identification of entities *within* each registry, it makes it very complex to properly map *between* Registries and more complex than necessary to map between registry identifiers and BICs. Adoption of LEI as a common identifier would not only improve this mapping, but also facilitate KYC information sharing between different KYC utilities.

SWIFT strongly supports the idea of requiring banks involved in correspondent banking to register for an LEI that can be used to identify them unambiguously and can be used to reference KYC information in all industry utilities. Such a standardised identifier would greatly simplify both information sharing and data aggregation.

To encourage this move we would recommend that all entities should be requested to create an LEI as part of their KYC utility onboarding; such LEIs could then also be re-distributed across different utilities. Were this work to be completed, it would have the additional benefit of ensuring that the correct legal entities (ie branches) can be properly identified at source, as opposed to their identification being tied to single BICs which often simply identify the parent companies or larger entities within which the individual legal entities sit.

In ISO 15022 securities messages a change has been accepted by the SWIFT and ISO standards communities to include a specific format for LEI identification of parties in addition to BIC and other representations. This change covers messages used for securities settlement and reconciliation, third-party collateral management and trade initiation and confirmation.

Whilst the addition of the LEI field in this relatively contained securities context is due to become effective in November 2016, we agree with the report's conclusion that it would be premature to consider adding an LEI field to the much more widely used payments messages at this stage. As the report suggests, once the LEI is more widely adopted, it would then be appropriate to see how this can be used within payment messages.

We also concur with the Committee's recommendation that BIC-LEI mapping can provide an effective bridge between the standards for many use cases.

Recommendation on the use of KYC utilities: The use of KYC utilities in general – provided that they store at least a minimum set of up-to-date and accurate information - can be supported as an effective means to reduce the burden of compliance with some KYC procedures for banks active in correspondent banking business. Relevant stakeholders (e.g. the Wolfsberg Group) may review the templates and procedures used by the different utilities and identify the most appropriate data fields to compile a data set that all utilities should collect as best practice and that all banks have to be ready to provide to banks which require the information.

As a provider of a KYC Utility for Correspondent Banking, SWIFT is a strong supporter of the concept of KYC Utilities and believes they can do much to reduce the cost and increase the effectiveness of banks' KYC operations.

SWIFT further agrees that standardisation of the baseline data set(s) and documents maintained in such utilities would lead to further efficiencies and savings at an industry level, given that it is unlikely that any single utility will emerge catering to all segments and use-cases. This sort of standardisation is in line with the baseline for correspondent banking that SWIFT defined together with its community, which is a global set of KYC data and documents.

Whilst banks concur that this is a very complete set of KYC information, they also recognise it will never cover 100% of their needs, since they will always have specific questions, depending on the specific nature of each client and the type of business they are engaged in. There will also inevitably be some variation in the KYC information required in different jurisdictions and markets, and variations in users' needs, depending on local policies, risk appetites, and so forth.

Standardising the baseline information will ensure the necessary uniformity needed by the industry. A number of KYC utilities have already emerged and it is likely that at least a few of these will continue to co-exist well into the future. It would be beneficial were these utilities to all collect a common set of basic information for each type of registered entity – and even for this information to be shared across these utilities. At the same time, it would also allow for individual utilities to extend and built upon the baselines to cater for distinct sectoral or market needs.

We believe that parties other than SWIFT would be better positioned to advise on the content of such a baseline definition. Further, we believe that such a definition would stand the best chance of widespread adoption if it were subsequently published and maintained by an independent standards organisation with an open governance structure. We therefore also recommend that should the industry agree on the need for a common standard, the effort be channelled through ISO Technical Committee 68 (Financial Services), in common with related standards in the field, including ISO 17442 (LEI).

Additionally, as data sets will differ marginally, depending on the type of entity (the on-boarding of a corporate client will require different information and transparency needs compared to a Financial Institution), it would be beneficial if a common taxonomy were also to be developed and adopted by all utilities. ISO would again be an optimal way of achieving this, whilst also providing a framework for evolution, in line with the changing regulatory landscape. For this reason, SWIFT has already started to look at evolving our KYC baseline to an ISO standard.

Developing these common standards and information baselines for all utilities would allow not only for more seamless information interchange and usage, but also for competition *between* utilities. Differentiation between the utilities would rest on their abilities and the mechanisms they offer to share additional documents on a bilateral basis, as well as other service adjacencies.

In addition to these standardisation recommendations, SWIFT has a further observation on the processes and procedures supporting the verification or qualification of the information submitted, and the frequency with which that information is checked.

Utilities like our own have put in place procedures to verify and qualify information, making sure that the information is as comprehensive and as complete as possible (whilst also ensuring we remain factual and do not perform any checks that are judgmental by nature). Ideally, users of those utilities that operate according to appropriately tight service descriptions should be able to rely on the information contained within the utilities, without having to re-do the related checks themselves. Absent a standard or form of assurance for KYC utilities, however, their ability to rely on the contained data may be limited. An independent standard governing the required process or assurance on the implementation of such a process, such as those that could be provided by ISO standard or an ISAE audit would be able to give such a guarantee.

Whilst it is important that the information is properly verified at the time that users first register with KYC utilities, it is equally important that the information is checked and maintained – and that the frequency with which such updates should take place is commonly agreed, adhered to and understood. An internationally agreed frequency level would therefore also be beneficial in this context, not least since it would appear that some entities need to know that the information has been re-confirmed within 90 days of their accessing the information, whilst other entities do not.

Recommendation on information-sharing initiatives: The work already conducted by the authorities with responsibility for AML/CFT (ie the Financial Action Task Force (FATF) and the Basel Committee on Banking Supervision AML/CFT Expert Group (AMLEG)) is very much appreciated. It is recommended that the FATF and AMLEG be invited to: (i) provide additional clarity on due diligence recommendations for upstream banks, in particular to what extent banks need to know their customers' customers ("KYCC"); (ii) further clarify data privacy concerns in the area of correspondent banking; and (iii) detail, to the extent possible, the type of data that information-sharing mechanisms could store and distribute in order to be a useful source of information.

In order to facilitate compliance with FATF customer due diligence recommendations, (i) the use of information-sharing mechanisms (if they exist in a given jurisdiction and data privacy laws allow this) for knowing your customers' customers could be promoted as the first source of information by default, which (ii) could be complemented bilaterally with enhanced information should there be a need.

In order to support information-sharing in general, the respondent bank may include provisions in its contractual framework with its customers (eg in the terms and conditions or in a supplementary agreement) which allow the bank to provide such information on request to other banks for AML/CFT compliance purposes.

As the Committee rightly acknowledges there are a lot of challenges around data privacy. It would be useful if it could be commonly agreed what *can* and what *cannot* be shared on given sets of information, and which mechanisms or controls should be put in place to allow for the storage and or exchange of more sensitive information. This could allow for the development of hybrid utility models in which only some data is centralised, being supplemented by the restricted data sets through secure information exchange between consenting participants.

---------- END ----------