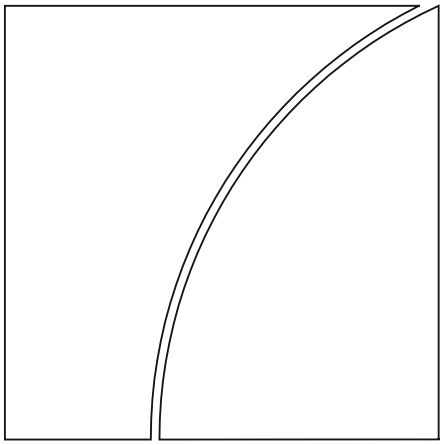
Committee on Payments and Market Infrastructures

Consultative report

Correspondent banking



October 2015

BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9197-244-9 (online)

Contents

Abbreviations

AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism
AMLEG	BCBS AML/CFT Expert Group
BCBS	Basel Committee on Banking Supervision
BIC	Business Identifier Code
CPMI	Committee on Payments and Market Infrastructures
ECB	European Central Bank
ECC	BIS Economic Consultative Committee
FATF	Financial Action Task Force
FSB	Financial Stability Board
GLEIF	Global LEI Foundation
GPFI	Global Partnership for Financial Inclusion
G-SIBs	Global Systemically Important Banks
ISAE	International Standard on Assurance Engagements
ISO	International Organization for Standardization
KYC	Know-your-customer
LEI	Legal Entity Identifier
LOU	Local Operating Unit (for the issuance and management of LEIs)
OFAC	Office of Foreign Assets Control
PMPG	Payments Market Practice Group
SME	Small and Medium-sized Entities

Executive summary

Through correspondent banking relationships, banks can access financial services in different jurisdictions and provide cross-border payment services to their customers, supporting international trade and financial inclusion.

In view of the importance of correspondent banking, the keen interest of central banks in this activity and the trends that point to risks to its safe and efficient functioning, the BIS Economic Consultative Committee (ECC) Governors have mandated the CPMI to produce a report on this issue. In response, the CPMI Working Group on Correspondent Banking has prepared this technical report describing current trends and analysing technical measures that might alleviate some of the concerns and cost issues related to correspondent banking.

Banks have traditionally maintained broad networks of correspondent banking relationships, but there are growing indications that this situation might be changing. In particular, some banks providing these services are reducing the number of relationships they maintain and are establishing few new ones. The impact of this trend is uneven across jurisdictions and banks. As a result, some respondent banks are likely to maintain relationships, whereas others might risk being cut off from international payment networks. This implies a threat that cross-border payment networks might fragment and that the range of available options for these transactions could narrow.

Rising costs and uncertainty about how far customer due diligence should go in order to ensure regulatory compliance (ie to what extent banks need to know their customers' customers - the so-called "KYCC"-) are cited by banks as among the main reasons for cutting back their correspondent relationships. To avoid penalties and the related reputational damage correspondent banks have developed an increased sensitivity to the risks associated with correspondent banking. As a consequence, they have cut back services for respondent banks that (i) do not generate sufficient volumes to overcome compliance costs; (ii) are located in jurisdictions perceived as very risky; or (iii) provide payment services to customers about which the necessary information for an adequate risk assessment is not available.

The regulatory framework, and in particular the AML/CFT requirements and the related implementing legislation and regulations in different jurisdictions, are taken as given in this report. It is acknowledged that these requirements, as agreed by the competent authorities, along with strict implementation, are necessary to prevent and detect criminal activities and ensure a healthy financial system.

The working group limited its analysis to technical measures that could help improve the efficiency of procedures, reduce compliance costs and help address perceived uncertainty, without altering the applicable rules and the basic channels for correspondent banking services between correspondent and respondent banks. The group analysed in detail some potential measures and translated them into four technical recommendations.

The working group believes that its recommendations might alleviate some of the costs and concerns connected with correspondent banking activities. However, the members are aware and would like to stress that, in isolation, these technical measures will not resolve all such issues. The working group acknowledges that the issues surrounding the withdrawal from correspondent banking are very complex and that costs related to AML/CFT compliance are only one of the elements that have to be considered in order to understand recent trends. Those include business considerations as well as economies of scope and scale issues. Limiting information challenges through the use of enhanced technical tools will only address part of AML/CFT compliance costs but does not resolve issues such as uncertainty about how far customer due diligence should go. In particular, the proposed technical measures will not immediately help the banks without access to correspondent banking services to gain such access.

In any case, all relevant stakeholders would need to be consulted before an implementation process for the recommended technical measures could start. This report is being published to seek public comment on these technical measures, by 7 December 2015, to be sent to the CPMI Secretariat (cpmi@bis.org). The comments will be published on the website of the BIS unless respondents have requested otherwise.

Recommendations:

- **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 (eg 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.
- **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 (eg 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.
- **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.
- **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.

1. Introduction

Correspondent banking is an essential component of the global payment system, especially for cross-border transactions. Through correspondent banking relationships, banks can access financial services in different jurisdictions and provide cross-border payment services to their customers, supporting, inter alia, international trade and financial inclusion. In addition, most of the payment solutions that do not involve a bank account at customer level (eg remittances), rely on correspondent banking for the actual transfer of funds. Until recently, banks have maintained a broad network of correspondent relationships, but there are growing indications that this situation might be changing. In particular, some banks providing these services are cutting back the number of relationships they maintain and are establishing few new ones.

In view of the importance of correspondent banking, the keen interest of central banks in this activity and the trends that point to risks to its safe and efficient functioning, the ECC Governors have mandated the CPMI to produce a report on this issue, especially as regards the potential measures to ensure an efficient provision of cross-border payment services globally. This report has been prepared by a designated CPMI Working Group on Correspondent Banking, which was set up to meet the ECC mandate, and has a technical character.

The main aim of this technical report is to elaborate on the payment system aspects of correspondent banking and to assess, from a technical perspective, the advantages and limitations of several measures that could facilitate the provision of correspondent banking services.

As the preparation of this technical report has faced significant time constraints, the following caveats need to be highlighted:

- The report is not based on a detailed fact-finding exercise. Participants in the CPMI working group gathered mainly qualitative information through interviews with selected institutions, but the report lacks a broad quantitative analysis. Moreover, the group did not gather feedback from non-CPMI jurisdictions, some of which may be among the most affected by the withdrawal from correspondent banking.
- The main conclusions and proposals have been shared informally with some industry groups. However, it needs to be highlighted that any potential recommendation to implement the measures described in this report requires further analytical work and should be preceded by a formal consultation process to avoid any unintended consequences.
- The CPMI has not liaised formally with other bodies and authorities that are active in this area, although some informal feedback has been sought from the Financial Action Task Force (FATF) and BCBS AML/CFT Expert Group (AMLEG).

  Some of the recent work and current initiatives in the area of correspondent banking are covered in Box 1.

Box 1

Initiatives on correspondent banking

Recent work and current initiatives in the field of correspondent banking by different international bodies and institutions include the following:

- **The Financial Stability Board (FSB)** is closely cooperating with the World Bank mainly to analyse the impact of the reduction of correspondent banking relationships on financial inclusion. In this respect, the *FSB Chair's letter to the G20 on financial reforms* of 9 April 2015 stated that "[…] the FSB has agreed a work plan that will examine […] together with the World Bank and other relevant bodies, the extent of potential withdrawal from correspondent banking, its implications for financial exclusion, as well as possible steps to address this issue."

- **The World Bank** is conducting surveys to better understand the evolution and drivers of bank account closures or restrictions, in the context of correspondent banking relationships and Money and Value Transfer services (remittances). Under the G20's Global Partnership for Financial Inclusion (GPFI), the World Bank collected information on whether and why far banks are terminating or restricting business relationships with remittance service providers. In partnership with the FSB and CPMI, the World Bank is leading another to obtain data on whether correspondent banking relationships are being terminated or restricted, the net effect of these developments and the underlying causes. This data-gathering will include non-CPMI jurisdictions.

- **The Financial Action Task Force (FATF)** issued two subsequent public statements on de-risking[1]in October 2014 and in June 2015 in order to clarify its approach to "de-risking", which is based on the risk-based approach as a central element of the FATF Recommendations. The risk-based approach requires financial institutions to identify, assess and understand their money laundering and terrorist financing risks, and implement AML/CFT measures that are commensurate with the risks identified. The June 2015 public statement on "de-risking" provides additional clarification on customer due diligence for correspondent banking relationships: "[…]When establishing correspondent banking relationships, banks are required to perform normal customer due diligence on the respondent bank. Additionally, banks are required to gather sufficient information about the respondent bank to understand the respondent bank's business, reputation and the quality of its supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action, and to assess the respondent bank's AML/CFT controls. Although there will be exceptions in high risk scenarios, the FATF Recommendations do not require banks to perform, as a matter of course, normal customer due diligence on the customers of their respondent banks when establishing and maintaining correspondent banking relationships[…]"..

  As a next step, the FATF agreed in June 2015 to undertake work to further clarify the interplay between the FATF standards on correspondent banking and other intermediated relationships, and the FATF standards on customer due diligence and wire transfers. In doing so, the FATF will consult with regulators and the private sector, and will take into account relevant work on correspondent banking and account closure being undertaken by the CPMI, the FSB, the Global Partnership for Financial Inclusion (GPFI), International Monetary Fund (IMF) and Union of Arab Banks (UAB), the World Bank Group, and the World Trade Organisation (WTO).

- **The Basel Committee on Banking Supervision (BCBS)** published in January 2014 its *Sound management of risks related to money laundering and financing of terrorism*, which contains an annex on correspondent banking (including money laundering/financing of terrorism risk assessments and customer due diligence requirements in correspondent banking).

Taking into account the complexity of this topic, a formal liaison to increase the coordination between the various work streams and the relevant authorities seems necessary in order to understand

[1] See www.fatf-gafi.org/topics/fatfgeneral/documents/rba-and-de-risking.html.

the many issues involved. Also the motivations of the main players vary and the impact of regulatory changes and the potential solutions to the problems need to be identified.

This technical report is organised as follows: after this introduction, Section 2 provides some basic definitions and outlines the main types of correspondent banking arrangements. It then summarises recent developments and touches on the underlying drivers. Section 3 sets out various technical measures that could facilitate correspondent banking, and weighs up their advantages and drawbacks. The final section concludes.

2. Developments in correspondent banking

2.1 Concept of correspondent banking

Correspondent banking can be defined, in general terms as "an arrangement under which one bank (correspondent) holds deposits owned by other banks (respondents) and provides payment and other services to those respondent banks".[2] The ECB uses a similar basic definition in its correspondent banking survey, referring to "agreements or contractual relationships between banks to provide payment services for each other."[3] A more detailed definition by the Wolfsberg Group[4] establishes that "[c]orrespondent Banking is the provision of a current or other liability account, and related services, to another financial institution, including affiliates, used for the execution of third-party payments and trade finance, as well as its own cash clearing, liquidity management and short-term borrowing or investment needs in a particular currency".[5] At the most basic level, correspondent banking requires the opening of accounts by respondent banks in the correspondent banks' books and the exchange of messages to settle transactions by crediting and debiting those accounts.

All these definitions highlight the main components of correspondent banking: a bilateral agreement between two banks by which one of them provides services to the other; the opening of accounts (by the respondent in the books of the correspondent) for the provision of services and the importance of payment services as a core function of correspondent banking. As the ECB definition highlights, these relationships are frequently reciprocal, in that each institution provides services to the other, normally in different currencies. Correspondent banking is especially important for cross-border transactions, as its importance for domestic payments within a single jurisdiction has diminished greatly due to the use of financial market infrastructures. On a cross-border level, however, correspondent banking is essential for customer payments and for the access of banks themselves to foreign financial systems for services and products that may not be available in the banks' own jurisdictions. This report analyses only cross-border correspondent banking activities[6] with a focus on payment aspects.

2 CPMI, "A glossary of terms used in payments and settlement systems", March 2003 (updated June 2015), www.bis.org/cpmi/publ/d00b.htm?m=3%7C16%7C266.

3 ECB, "Ninth survey on correspondent banking in euro", February 2015, www.ecb.europa.eu/pub/pdf/other/surveycorrespondentbankingineuro201502.en.pdf.

4 The Wolfsberg Group is an association of 13 global banks which aims to develop guidance and frameworks for the management of financial crime risks with respect to KYC, AML and CFT policies.

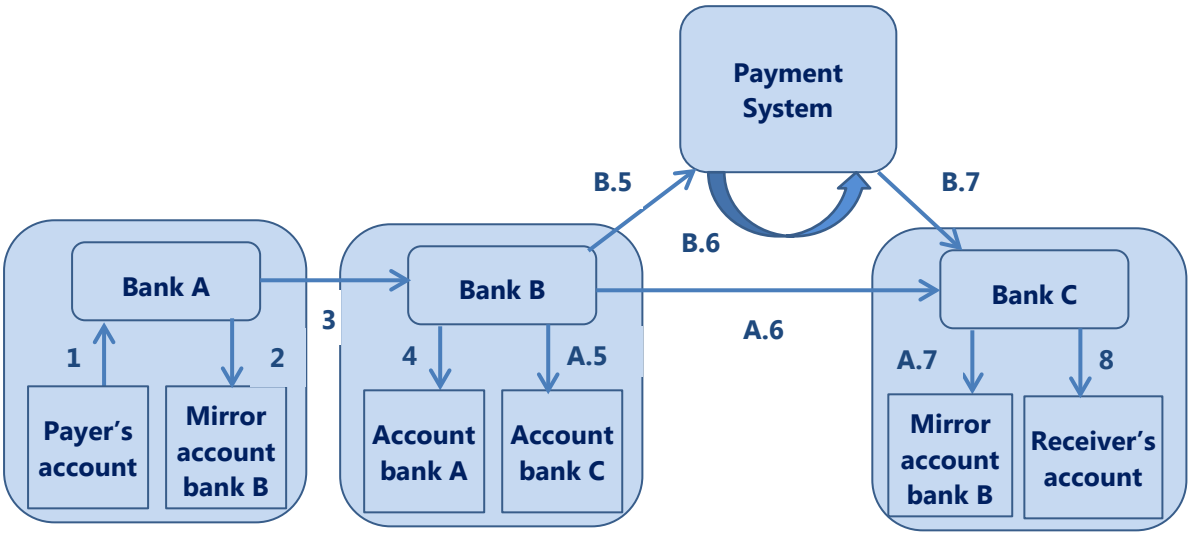
5 The Wolfsberg Group, "Wolfsberg Anti-Money Laundering Principles for Correspondent Banking", 2014, www.wolfsberg-principles.com/pdf/home/Wolfsberg-Correspondent-Banking-Principles-2014.pdf.

6 Some innovative payment service providers, including non-banks, offer services that could be an alternative to correspondent banking for specific types of retail payments. These types of services and providers have been analysed in previous CPMI reports (*Innovations in retail payments* (2012) and *Non-banks in retail payments* (2014)).

The figure below sketches out the main flows involved in correspondent banking payments and the interplay between correspondent banking services and payment systems. It shows the settlement of a payment from bank A to bank C via a correspondent bank. As banks A and C do not hold accounts with each other, they use the services of bank B as intermediary. In one case, bank B transfers the payment to C using correspondent banking only, whereas in the other, bank B uses a payment system in which both B and C participate for transferring the payment. A, B and C would normally be located in two or more different jurisdictions and there could be other banks involved on the sending and receiving sides (as intermediaries in the correspondent banking chain).

Figure 1

Payments settled via correspondent banking



1. Debiting of payer's account with bank A
2. Crediting of bank B's mirror account with bank A, which is kept for accounting purposes
3. Payment message from bank A to bank B via telecommunication network
4. Debiting of bank A's account with bank B (loro account)

A. Use correspondent bank only

5. Crediting of bank C's account with bank B
6. Payment message from bank B to bank C via telecommunication network
7. Debiting of bank's B mirror account with bank C, which is kept for accounting purposes
8. Crediting of receiver's account with bank C

B. Involvement of payment system

5. Payment message from bank B to payment system
6. Settlement via payment system
7. Payment message from payment system to bank C
8. Crediting of receiver's account with bank C

Source: ECB, *Ninth survey on correspondent banking in euro,* 2015, adapted from Danmarks Nationalbank, *Payment systems in Denmark*, 2005.

Correspondent banking may include various services, such as international funds transfers, cash management services, check clearing, loans and letters of credit or foreign exchange services. There are several ways of providing these services:

- In traditional correspondent banking, a respondent bank enters into an agreement with the correspondent bank in order to execute payments on behalf of the respondent bank and its customers. The respondent bank's customers do not have direct access to the correspondent account, but they transact business indirectly.
- Nested correspondent banking refers to the use of a bank's correspondent relationship by a number of respondent banks. The latter have no direct account relationship with the

correspondent bank but conduct business through their relationships with the bank's direct respondent bank to execute transactions and obtain access to other financial services (eg a local bank conducts correspondent banking business indirectly via its regional savings bank).

- Payable-through accounts, also known as "pass-through" or "pass-by" accounts, are similar to nested correspondent banking but, in this case, the respondent bank allows its customers to directly access the correspondent account to conduct business on their own behalf.

2.2 Recent developments in correspondent banking

As correspondent banking services are a key element in cross-border transactions, they might be expected to grow in parallel with the expansion of international trade and cross-border financial activity. However, there are increasing indications of an overall cutback in the number of correspondent banking relationships and, for smaller banks in some specific jurisdictions, difficulties seem to exist in establishing new relationships. In particular, during the informal fact-finding carried out by the CPMI working group the following trends have been identified:

- Cutbacks in the number of relationships: Correspondent banking relationships are being reduced in number, especially for respondent banks that (i) do not generate sufficient volumes to recover compliance costs; (ii) are located in jurisdictions perceived to be very risky; or (iii) provide payment services to customers about which the necessary information for an adequate risk assessment is not available.
- Changes in relationships: Those types of correspondent banking services that are perceived to have higher associated risks (nested correspondent banking, payable-through accounts) are being scaled back, so that traditional correspondent banking clearly predominates in the remaining relationships. These remaining relationships are often retained only to support the cross-selling of other products to respondent banks (ie the profit is made in other business areas and correspondent services are considered as a necessary ancillary service).
- Concentration of relationships: Cutbacks in the number of relationships as well as changes in their nature have resulted in a significant concentration of relationships in a relatively small number of service-providing institutions, which increasingly dominate this market. In addition, a concentration of correspondent banking activities within affiliated banks was observed.
- Increasing costs: The establishment and maintenance of a correspondent banking relationship are perceived to be increasingly costly both for correspondent and respondent banks.
- Cutbacks to correspondent banking services in specific foreign currencies: Some correspondent banks are increasingly reluctant to provide correspondent banking services in certain foreign currencies in which the perceived risk of economic sanctions, the regulatory burden related to AML/CFT or the uncertainties related to the implementation of these requirements and the potential reputational risk in case of non-compliance seem to be higher. There are indications that correspondent banking activities in USD are increasingly concentrated in US banks and that non-US banks are increasingly withdrawing from providing services in this currency except for some ancillary services. Simultaneously, the very same non-US correspondent banks might still be willing to provide correspondent banking services in their domestic currency.
- Geographical imbalances: Not all jurisdictions and currencies are affected equally. Respondent banks, in particular smaller banks located in jurisdictions perceived to be very risky, are especially affected by the reduction in the number of relationships.

What are the drivers that can explain these recent trends? From the demand side, at least some respondent banks are actively reducing the number of correspondent banking relationships in order to

reduce their own risk management work, simplify reporting of intraday liquidity, concentrate their payment channels and cut costs. However, a significant demand for these services still seems to exist.

Most of the drivers seem to derive from the supply side (ie correspondent banks providing the service to respondent banks). One of the main drivers seems to be the growing tendency for banks to assess the profitability of their business lines, customers and even jurisdictions in a world where capital and liquidity are scarcer and more expensive. While the correspondent banking business seems profitable in aggregate, parts of this business are not and, as a result, correspondent banks have been dropping their less profitable customers or jurisdictions. This is especially true where the business returns do not justify the cost of investment. According to the correspondent banks interviewed for this report, the most common cause for this reduction of profitability is the increasing cost of regulatory compliance, especially in relation to AML/CFT regulation. According to anecdotal evidence these costs have reached such a level that, for certain financial institutions, there is no business justification for continuing to engage in correspondent banking. In addition to the increased compliance costs, interviewed banks mentioned also the high degree of uncertainty as to what exactly constitutes compliance with the requirements in order to avoid penalties and related reputational damage. For example, some of the interviewed banks believe that it is necessary to "know your customers' customers (KYCC)", and there seems to be a degree of uncertainty as to when this is necessary and how detailed this knowledge should be. This uncertainty increases the difficulty of measuring the risks associated with correspondent banking and might be leading to the abandonment of some relationships. However, not all the causes seem to be directly related to increasing regulatory costs: the general trend of financial institutions to downsize and deleverage in the wake of the financial crisis seems to be behind the decisions of some correspondent banks to eliminate or scale back this line of business, particularly if it is not considered a core activity. Also, country risk (geopolitical and financial) may have increased, so that the rising costs may be due partly to the application of existing policies to a larger number of high-risk countries, not just to higher enforcement activity and penalties.[7]

In summary, increasing costs, regulatory pressure and an increased perception of risk are reducing the profit margins associated with this activity in some countries and/or with some customers and could be making this line of business increasingly unappealing to a growing number of correspondent banks. In particular, this is a business highly influenced by economies of scale where banks are struggling to make returns when the business volumes in certain jurisdictions and/or with certain customers are not considered to justify the compliance costs involved. The perception is that this line of business has shifted from being a low-risk/low-margin segment to a high-risk/low-margin one.

Not all correspondent banks are reacting in the same way and not all respondent banks are being affected equally by these developments.

Some correspondent banks are specialising in the provision of correspondent banking services as a source of profit, and are thus focusing on respondent banks that provide a business volume that is sufficient to justify the increasing costs (including fixed costs) and which are located in jurisdictions perceived to constitute an acceptable level of risk. These banks consider the increased complexity in the correspondent banking business as a challenge but at the same time as an opportunity to increase their competitive advantage. However, the majority of institutions seem to be maintaining existing correspondent banking services only insofar as these services are necessary to serve the needs of

[7] From the regulatory side, no significant changes in AML/CFT have been introduced recently and banks are expected to continue applying a risk-based approach for their customer due diligence in relation to AML/CFT. There are indications, however, that in some instances the perception of the ML-FT risks associated with activities, such as correspondent banking, is changing. The term "de-risking" is commonly used to refer to those instances in which banks adopt "increasingly stringent financial crime-related policies to reduce their exposure to potential money laundering, terrorist financing, corruption and sanctions risk". (*De-risking: Global Impact and Unintended Consequences for Exclusion and Stability*, The Wolfsberg Group and other contributors, 2014).

corporate customers for cross-border payments and trade finance or to support the cross-selling of other products to respondent banks (ie the profit is made in other business areas and correspondent services are considered as a necessary ancillary service) or to preserve reciprocity in their correspondent relationships. As a result, respondent banks that fit within any of these business strategies are likely to maintain relationships, whereas others might risk being cut off from the international payment networks. Banks which might risk losing access to correspondent services tend to be smaller institutions that do not generate volumes considered to be sufficient, that are located in jurisdictions perceived to be very risky, that are not part of an international group or that provide payment services to customers about which the necessary information for an adequate risk assessment is not available.[8] This trend implies a risk that cross-border payment systems will fragment, reducing the available options for these transactions.

This division of banks into groups which are more likely to maintain correspondent relationships and those which are not could also explain the apparent contradiction between the observed reduction of relationships and the reduction of margins in parts of the market. Usually a reduction of relationships would give banks specialised in providing correspondent banking services substantial market power, but the reduction of profit margins shows that such banks are unable to pass increased compliance costs on to their respondent banks. This in turn suggests that the market is still competitive or that compliance risks are not adequately priced. Consequently, competition may still be quite vigorous in some segments of the market (relatively larger players, low-risk jurisdictions) but at the same time supply (at any price) may have been reduced or completely shut off for other players (smaller institutions, high risk jurisdictions), which might effectively isolate these players from the international markets.

All in all, it seems that many of the correspondent service-providing banks interviewed in the CPMI jurisdictions are adapting their business model by taking into account the increasing costs, the regulatory requirements and risk management considerations, although some have exited the market voluntarily because of the lack of a business case. Despite these changes on the supply side, most banks are able to obtain cross-border payment services. Nevertheless, banks in some jurisdictions have lost their ability to make cross-border payments. As mentioned above, however, this evolution in correspondent banking seems to have most severely affected smaller banks and/or banks that are located in jurisdictions considered to be very risky.

3. Potential measures to facilitate correspondent banking services

3.1 General considerations

In view of the trends described above, several measures that could facilitate compliance with regulatory requirements applicable to correspondent banking services have been identified. This section elaborates on the advantages and drawbacks of these measures, leading to the identification of several potential high-level recommendations that could facilitate the provision of correspondent banking services. These potential measures are: (i) Know-your-customer (KYC) utilities; (ii) increased use of the LEI; (iii) information-sharing mechanisms; and (iv) improvements in payment messages.

The analysis below aims to describe the technical measures and explains how they could help to increase the efficiency of procedures and reduce compliance costs without altering the applicable rules and the basic channels for correspondent banking services between correspondent and respondent banks. In addition, the existing regulatory framework is taken as given. Although these technical

[8] Some institutions report providing correspondent banking services only to affiliates within their banking group.

measures might alleviate some of the costs and concerns connected with correspondent banking, it needs to be stressed that, in isolation, they will not resolve all such issues. The issues surrounding the withdrawal from correspondent banking are very complex and costs related to AML/CFT compliance are only one of the elements that have to be considered in order to understand recent trends. Those include business considerations as well as economies of scope and scale issues. Limiting information challenges through the use of enhanced technical tools will only address part of AML/CFT compliance costs but does not resolve issues such as uncertainty about how far customer due diligence should go. In particular, the proposed technical measures will not immediately help the banks without access to correspondent banking services to gain such access.

It can be argued that the industry itself should manage its costs and revenues, and identify and implement solutions that will increase the efficiency of correspondent banking as necessary. However, the smooth functioning of the international correspondent banking market is essential to facilitate global trade and financial transactions across jurisdictions. Since individual banks' decisions to withdraw from correspondent banking can disrupt the functioning of the entire market, their individual decisions may entail a negative externality for the correspondent banking network. At the same time, individual actors may face a considerable degree of uncertainty and high investment costs with regard to implementing dedicated solutions. Moreover, they may encounter a substantial coordination problem, as there might be a first-mover disadvantage in implementing some of these measures. As a result, public authorities, as well as other relevant stakeholders (ie Wolfsberg Group and PMPG[9]), may promote the implementation of these solutions to reduce the uncertainty and to solve the coordination problem, thereby contributing to an increase in the overall efficiency of correspondent banking so as to reduce negative externalities. It has to be stressed, however, that due to the study's limitations, any potential implementation of the measures described in this technical report through recommendations needs to be preceded by a formal consultation process and requires further analytical work to gauge the potential impact of any measure so as to avoid unintended consequences.

3.2 KYC utilities

Know-your-customer (KYC) due diligence is an essential element of banking, including correspondent banking. Customer due diligence is applied by all banks providing a service in the correspondent banking chain to the institutions or customers with which they directly interact. This section focuses on the KYC activities performed by correspondent banks on their respondent banks (KYC activities performed by respondent banks on their customers are not specific to correspondent banking and are not covered in this section).[10]

Customer due diligence requires that correspondent banks identify and understand their respondents' banking activities and know if the respondents maintain additional correspondent banking relationships.[11] This process often leads to a massive exchange of documents. According to SWIFT, the

[9] The Payments Market Practice Group (PMPG) is an independent body of payments experts from Asia-Pacific, Europe and North America which acts as an independent advisory group. The PMPG aims, inter alia, to take stock of payments market practices across regions, discuss, explain and document market practice issues and recommend market practices and best practices, business responsibilities and rules.

[10] Current expectations in correspondent banking include that correspondent banks extend their customer due diligence on respondent banks (KYC) to include also a deeper monitoring and understanding of the underlying correspondent banking transactions and possibly the identities of the originator and final beneficiary. This approach is informally referred to as "know your customer's customer" ("KYCC"). These types of expectation are covered in Section 3.4 on information-sharing arrangements.

[11] The customer due diligence process should not be a "paper-gathering exercise" but a real assessment of ML risk (see BCBS paper on Sound management of risks related to money laundering and financing of terrorism, 2014, Annex 2).

7,000 banks that use the SWIFT network for correspondent banking have more than 1 million individual relationships, so the number of documents exchanged is presumably much higher.[12]

This setup creates several problems: first, the same or very similar information needs to be sent to all correspondents; second, correspondents may have differing information requirements, as this is a risk-based process that is not standardised. Finally, it has to be taken into account that information is exchanged not only at the outset of a relationship, but that continuous updates are necessary. As a result, the KYC due diligence process is complex, costly, time-consuming and labour-intensive.

To improve this situation, several providers have developed or are developing KYC utilities, with the aim of storing in a single repository relevant due diligence information. These utilities may help correspondent banks to identify and mitigate the risks associated with respondent banks. Respondent banks would access such a utility to provide the initial information and then provide updates as necessary in line with a standardised template, whereas correspondent banks would access it to retrieve the necessary information. Information-providing banks (respondents) maintain full control over their data and determine which banks have access to it.

The use of KYC utilities would provide several advantages: (i) the number of times a bank must send the same information could be greatly reduced; (ii) the accuracy and consistency of the information could improve, as banks would only maintain one set of updated information; (iii) the use of a single template might promote the standardisation of the information that banks provide to other institutions as a starting point for KYC obligations; (iv) the use of a central KYC utility might speed up the process; and (v) costs could be reduced thanks to a lesser amount of documentation being exchanged. In view of this, authorities may wish to promote the use of KYC utilities.

Banks' costs could be further reduced if they were able to place more reliance on KYC utilities so that they could undertake fewer checks of the quality of data held in the utilities. One way to achieve this might be to establish some form of independent standard to set out what systems and controls such utilities should have to ensure that the data they hold are accurate and to facilitate some form of external accreditation process to test compliance with this standard. It is unlikely that central banks could do this but there could be a role for other authorities, bodies (eg ISO or ISAE standards) and external auditors in facilitating this.

In summary, the information in this type of utility might be a good starting point for KYC due diligence processes by correspondent banks. Box 2 includes a brief description of some of the main KYC utilities.

Box 2

A brief description of some KYC utilities

Bankers Almanac

This utility focuses on financial institution KYC and is therefore designed to meet the needs of correspondent banking. In order to be included, financial institutions must be able to demonstrate a legitimate physical address, appropriate licences and a confirmation that they are regulated by a regulator of international repute. Ahead of publication, all data collected are quality-assured by a content team at Bankers Almanac.

Depository Trust & Clearing Cooperation (DTCC) – Clarient Entity Hub

The Clarient Entity Hub went live in February 2015. The scope of this utility is broad and covers investment managers, hedge funds, corporates and banks. It allows for a secure upload, storage, categorisation and distribution

[12] SWIFT KYC registry factsheet, December 2014, http://complianceservices.swift.com/sites/complianceservices/files/kyc_registry_factsheet_december_2014.pdf.

of data. The provider of the data has the right to grant access to its data and therefore always controls on a granular level who has access to the information. Clarient Entity Hub facilitates standardisation and at the same time provides the flexibility to share documents above and beyond Clarient's standards on a bilateral basis. Clarient supports the sharing and management of different types of data and documents such as KYC, TAX, Ops data and other client related documentation. Clarient leverages current compliant reference data from DTCC's established set of customer reference data services. The information provided is validated by Clarient in order to produce the so-called "golden record". This verification is done by linking each data element to evidentiary documentation. In case inconsistencies are detected these are flagged to the customer for checking.

Markit | Genpact

The Markit/Genpact KYC Service was launched in May 2014. This service covers banks, asset managers, corporates and hedge funds. It builds on expertise and technologies offered by Markit and Genpact, including Genpact's Remediation as a service platform, which offers transparent workflow, document management, analytics, reporting, traceability and governance, and Markit's Counterparty Manager Service. The service standardises and centralises the collection and management of KYC data for financial institutions in order to streamline customer onboarding. Legal entity data and documents that banks require from their customers in order to conduct business and comply with KYC and anti-money laundering regulations are collected, enriched and centrally administered. Entities are identified once globally and maintained according to an industry-defined standard, consistent with subscribing bank policies for onboarding. The service will actively monitor customer information. Access to up-to-date customer reference data is provided due to proactive data revalidation on regular schedules (ie annual refresh cycles).

SWIFT KYC Registry

The SWIFT KYC Registry went live in December 2014. It focuses on banks active in correspondent banking, but not on customers. The SWIFT KYC Registry allows banks active in correspondent banking to use a central utility to provide information needed for compliance requirements. This information can be used by correspondent banks to conduct adequate due diligence with regard to their customers (ie the respective respondent bank). All information stored is checked and validated by a dedicated operational team at SWIFT. Each bank that provides data always retains the ownership of its data. Other banks can only access data of another bank when permission to do so has been granted by the data-owning party. In addition, SWIFT is also introducing the so-called "SWIFT Profile". This profile provides a standardised portrait of a bank's traffic activity with sanctioned or high risk countries (as per FATF/OFAC/EU lists) on SWIFT. Banks can share this profile with selected counterparties by using the SWIFT KYC Registry.

Thomson Reuters Accelus

Accelus Org ID went live in March 2014. The customer records cover hedge funds, asset managers, corporations and banks active in correspondent banking. The customers submit documentation and actively authorise access to the information. A party always keeps full control and visibility over who can access and view the respective party's documents. Accelus Org ID validates the information, adds public data and scores the customers according to risks. Accelus Org ID protects data privacy in a secure environment with constant monitoring to ensure that records are up-to-date and information is accurate. With regard to correspondent banking, Accelus Org ID standardises document requirements through its globally agreed KYC policy and alignment with the Wolfsberg principles.

Source: Publicly available information.

In principle, the implementation of KYC utilities is a positive development. However, there are some limitations that have to be acknowledged:

- KYC utilities may facilitate the access to a basic set of information, but they do not alter the basic responsibility of correspondent banks to perform due diligence on their customers (ie the respondent banks). Correspondent banks cannot simply delegate their responsibility as KYC utilities cannot perform due diligence on behalf of third parties and the ultimate responsibility

always lies with the correspondent banks.[13] Thus, even if KYC due diligence procedures are facilitated, resources will still be necessary for the analysis and management of the risks involved in a relationship.

- KYC utilities use agreed templates, but templates differ across utilities.
- KYC utilities may not collect all the information that a correspondent needs for its internal assessment. Additionally, these processes cannot be easily standardised, as they are risk-based. The data stored in a KYC utility would need to be complemented with additional data transmitted bilaterally, and thus these utilities should be seen more as a useful starting point for due diligence obligations rather than as eliminating the need for due diligence by the correspondent bank.
- KYC utilities need to be updated routinely by the respondent bank with fresh information in order to remain useful to the correspondent bank for the ongoing monitoring of an existing relationship or for the opening of a new relationship. Providers of the KYC utilities need to set adequate parameters regarding which events will trigger a requirement to update information.
- The privacy laws of some jurisdictions may prohibit sharing, storing or mining of basic information in KYC utilities, such as other correspondent relationships and details of geographical areas served. Operators of KYC utilities need to check carefully and in line with applicable laws what information should and could be shared in the KYC utilities, especially when information is transmitted across borders.
- Additionally, to the extent that some institutions are not participating in any utility, there would be a need to maintain bilateral exchanges of information. In order to increase efficiency, both respondent and correspondent banks need to have access to a utility with a broad coverage of relevant participants. While KYC utilities may facilitate customer due diligence on respondent banks, they may not address all information needs related to where a respondent does business and with whom (see Section 3.4 for an analysis of these problems).

In summary, KYC utilities are a promising tool for speeding up KYC compliance and cutting its costs. Although a complete standardisation of the information seems unfeasible (especially due to the risk-based approach for AML/CFT), the utility template, if designed appropriately could help defining an acceptable minimum set of data that any bank should be ready to provide to banks requiring the information. This minimum set of information could be augmented bilaterally as necessary.

Recommendation: 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 (eg 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.

[13] As correspondent banks cannot delegate their basic responsibilities in this area, in some jurisdictions correspondents are reluctant to use these facilities as it is considered that the information stored in these utilities is not always updated or correct.

3.3 Legal Entity Identifier (LEI)

3.3.1 General information on the LEI

In the wake of the financial crisis, the importance and benefit of an unambiguous Legal Entity Identifier (LEI) became clear. Authorities worldwide acknowledged their inability to clearly identify parties to transactions across markets, products and regions. This hampered the ability to evaluate emerging risks, including systemic risk, as well as to identify trends, thus preventing stakeholders from being in a position to take corrective steps. Consequently, authorities, in close collaboration with the private sector, have developed a framework that allows for the unambiguous identification of entities through the issuance of unique LEIs, which may be also used for reporting and other regulatory purposes in the various jurisdictions.

Box 3

Basic background information on the LEI and current issuance status

The LEI (ISO standard 17442:2012) is a 20-digit alphanumeric reference code to unambiguously identify legal entities that engage in financial transactions. Each LEI is assigned to a unique legal entity and each legal entity may have only one LEI. The LEI code is associated with reference data, currently including basic identification information, such as the official name of the legal entity and the address of its headquarters. It is expected that the standard will be enhanced in the future so that the reference data will also include the direct and ultimate parent(s) of legal entities and also information on relationships (including ownership). It is important to highlight that the LEI is envisaged for the unambiguous identification of legal entities (and trusts), but is not applicable to natural persons. The LEI is not intended to be a source of AML information, nor is it used as a routing code for cross-border payments (instead, the Business Identifier Code (BIC) is widely used for this purpose).

LEIs are issued in various jurisdictions through Local Operating Units (LOUs), which issue LEIs against a fee and validate the reference data upon issuance and following periodic certifications. LOUs make the LEIs and the associated reference data publicly available free of charge. Once a legal entity has obtained an LEI, it cannot obtain another, but it can transfer the maintenance of its code from one LOU to another. The coordination of the LEI system on a global basis is done via the GLEIF (Global LEI Foundation),[14] established in 2014 as a not-for-profit organisation, which coordinates the activities of the LOUs and supports the maintenance of the centralised database of identifiers and related reference data.

As of end-2014, more than 330,000 legal entities from 189 countries had obtained LEIs from the 20 operational LOUs endorsed for issuing globally compatible codes after meeting defined standards. The current usage of the LEI focuses mainly on derivatives transaction reporting and other regulatory reporting issues (eg the European Banking Authority (EBA) recommends the LEI as unique identification code for supervisory purposes for every credit and financial institution in the European Union).

3.3.2 LEI and correspondent banking

Correspondent banking requires a robust mechanism for identifying the parties involved in payment processing for a variety of reasons: risk management, regulatory requirements and in particular the smooth processing (eg clear routing information to ensure straight through processing). Whereas the BIC is the de facto standard for the latter, one of the elements that can be considered for the first two reasons, especially to facilitate AML/CFT screening, may be the use of the LEI as a means of identifying the parties to a transaction. The LEI system focuses on providing a standardised identification and a

[14] See www.gleif.org/en.

centralised database from which information can be retrieved easily. It does not process or record financial transactions. Although the LEI system has not been designed to facilitate AML/CFT compliance in correspondent banking, its use may bring some benefits in this area:

- The LEI may be used to improve the effectiveness of some of the measures described in this report. In particular, KYC utilities and information-sharing mechanisms described in Sections 3.2 and 3.4 require an unambiguous identification of the banks or customers included in the respective databases. Rather than developing a specific standard for this purpose, the LEI can be promoted as an efficient global standard for these utilities.
- The LEI's widespread use could help financial institutions to identify specific entities unambiguously and increase the effectiveness of automatic screening packages, particularly for identifying sanctioned entities (eg by reducing the number of "false positives" when screening names and addresses that only partially match the data of a given entity).
- It may also facilitate the consolidation of information received in financial intelligence units, by identifying transactions of the same entity reported by different financial institutions more easily.
- The LEI may also become an option for supporting the implementation of specific FATF recommendations, such as recommendation 16[15] on the provision of originator and beneficiary information in payment messages.[16] The information required by this recommendation could be communicated in different ways, but the LEI's use within payment messages when the originator and/or beneficiary are legal entities might be an additional way of complying with the requirement in the future.

Nevertheless, it should be noted that the LEI is not a panacea for cross-border correspondent banking services. In particular, the following limitations need to be highlighted:

- The LEI does not apply to individuals, and so alternative means of ensuring a clear identification of natural persons in line with the FATF recommendations[17] are needed in correspondent banking transactions. These methods will also need to comply with data protection legislation.
- If and when the reference data are expanded, the LEI will provide information on ownership and relationships between legal entities. This information, however, will also be limited to legal entities, and will thus not cover the identification of natural persons as beneficial owners of legal entities, which is one of the main aims of AML/CFT requirements.
- The use of the LEI is helpful as a way of unambiguously identifying legal entities and avoiding confusion, but the standard is not geared towards the identification of counterparties from an AML perspective. The LEI's use might facilitate part of the customer due diligence processes (eg by determining more easily that an entity is already a customer and by avoiding the duplication of due diligence efforts and records) but it has to be clear that the use of the LEI is not a substitute for customer due diligence and that banks remain responsible for adequate customer due diligence, given that the LEI system was not designed as a means of performing customer due diligence on behalf of third parties.
- Up to now, it has not been foreseen that the payment messages used in the correspondent banking business (eg MT 103 or equivalents) would include either a dedicated field/line or a

[15] FATF recommendation 16: "Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain".

[16] Section 3.5.3 elaborates on the potential use of the LEI in payment messages.

[17] See FATF recommendations INR16.

dedicated code for including the LEI in the payment messages (see Section 3.5). Moreover, the routing of payments is based on BICs; currently other information that provides for adequate customer due diligence is included within the payment message (ie the information included is in line with the FATF recommendations).

Considering the above advantages and limitations, the following can be concluded:

- The use of the LEI to identify the banks involved in a correspondent banking relationship does not seem to pose an unsurmountable challenge, as the number of entities involved is limited and, in any case, banks are likely to obtain an LEI code for other purposes (eg for regulatory reporting and reporting of OTC derivatives to trade repositories). This would promote the usage of the LEI and contribute to the aim of clearly identifying parties to transactions across markets, products and regions. The additional benefits, however, would be limited, as the counterparties are usually well known to each other and other identifiers are needed in any case for routing purposes (eg the BIC).
- Whereas the LEI aims at unambiguously identifying legal entities, BICs are the cornerstone of the global payments network as they are the basis for all message routing. Therefore, the IT applications of banks active in correspondent banking business are programmed around BICs. Banks send messages to each other by populating the payment message with the relevant BICs. By using BIC to LEI mapping utilities (such as SWIFT's BIC to LEI directory, which will be replaced by the SWIFTRef Entity Plus directory) it is possible to map the information of BICs and LEIs. This ensures an unambiguous and efficient identification of the banks involved in the payment chain at any time.
- The use of the LEI to identify a bank's customer seems much more challenging, as the sheer number of legal persons/corporates concerned is vastly higher than that of the correspondent banks involved. This challenge also highlights the potential benefits, as a clear identification of originator and beneficiary would be advantageous to all involved banks, although it has to be acknowledged that these benefits would be limited to the identification of legal entities. Furthermore, the current design of payment messages such as MT 103 (or equivalents) does not foresee the provision of the LEI in fields containing information on the ordering customer/final beneficiary but is geared rather to the provision of other information in line with FATF recommendation 16. Therefore, the current message design provides for the information needed to identify each and every customer – corporates as well as natural persons – without the need to specify an LEI.

In a nutshell, the increased use of the LEI in correspondent banking services is seen as a positive development that might well be used in combination with some of the technical measures described in Sections 3.2 and 3.4 of this report, which focus on the provision of information. It is expected that, especially due to forthcoming regulatory requirements, the future use of the LEI will increase significantly in various segments of the financial markets.

The LEI's use in correspondent banking can benefit from the increased use of the standard in other segments of the financial markets and could in turn reinforce the worldwide demand for the LEI. Any requirement or recommendation to use the LEI in cross-border correspondent banking should be coordinated in order to be effective and to solve potential coordination problems. However, it should be noted that the LEI is a means of identification, not a routing criterion in the payment chain, and cannot substitute for the BIC without very significant changes to banks' payment applications. By using mapping facilities, banks will always be in a position to retrieve the corresponding LEI when only the BIC is provided.

With regard to the identification of customers and especially for corporates, using the LEI for the identification of the ordering customer and the final beneficiary could also be encouraged as a long-term goal.

Nevertheless, it should be acknowledged that there is no LEI for individuals[18] and that, currently, sufficient information for customer due diligence can already be provided in the message without necessarily including the LEI. Therefore, in order to avoid any unintended consequences, it seems advisable to await a more widespread usage of the LEI by such entities before considering any changes to the information that should be included in a message (see also Section 3.5.3 on the potential inclusion of the LEI in the payment message).

Finally, it is acknowledged that the LEI's use as a means of identification will not totally solve the challenges associated with correspondent banking, although it could improve the effectiveness of some technical measures (in the same way as KYC utilities or information-sharing initiatives), at the same time reinforcing other public policy objectives related to the use of the LEI in other areas.

Recommendation: 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 (eg 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.

3.4 Information-sharing

Under certain circumstances, such as with jurisdictions or customers that are seen as higher risk for money laundering, the correspondent bank's due diligence obligations go beyond KYC on the respondent bank (ie the direct customer of the correspondent bank). In some cases correspondent banks would need to know with whom and where its respondent does business, possibly including the identity of its respondent bank's customers, both at account and payment level. Consequently, correspondent banks should monitor in depth and thoroughly understand the underlying transactions. Correspondent banks need strong activity monitoring systems to detect suspicious transactions and may need access to extended information on the originators and beneficiaries related to such transactions. Authorities expect a correspondent bank to conduct sufficient due diligence to understand and mitigate risk and, at times, this may entail a better understanding of whom its customer does business with and where (including when a bank is acting as intermediary). A correspondent bank's efforts to obtain information on its customer's customer are informally referred to as "KYCC" (know your customer's customer).[19]

This expectation increases the security of correspondent banking, but it also increases the complexity of AML/CFT procedures, owing to the following main difficulties and consequences:

- The most significant problem is that this expectation may implicitly entail that respondent banks are in a position to easily provide additional transaction and customer information to correspondent banks. In many jurisdictions, however, these requirements can conflict with data privacy laws. If respondent banks cannot provide additional information on customers and specific transactions for this reason, correspondent banks may have no alternative but to block or reject suspicious transactions. This could eventually lead to the termination of some

[18] Although there are some initiatives which allow eg trading "individuals" to obtain an LEI (see the United Kingdom's Sole Trader regime), it is not currently foreseen that individuals would be identified by means of LEIs.

[19] See FATF, "De-risking; Global Impact and unintended consequences for exclusion and stability", discussion paper; prepared for use by the October 2014 FATF Plenary and associated working groups. "In addition an increasing expectation that banks providing correspondent services must "Know your Customer's Customer" has added a further level of complexity and difficulty."

correspondent banking relationships, particularly in jurisdictions with restrictive data privacy laws.

- Even if correspondent banks have access to additional information on specific transactions, it is very difficult in many cases for an upstream bank to check the identities and purpose of the transactions, as they do not have direct contact with the customers, which are also normally located abroad. With the exception of a clear match with identities or jurisdictions included in a few well known international lists,[20] a correspondent bank may find it difficult to obtain reasonable assurance about a transaction's legitimacy. This introduces an element of uncertainty that makes this type of due diligence processes difficult to fulfil. Taking into account the uncertainty and the difficulty involved in evaluating risks, some banks may decide to withdraw from correspondent banking altogether, or terminate relationships with respondent banks that generate low volumes of operations or are located in jurisdictions perceived as high risk.
- As many respondent banks have multiple correspondent relationships, there will be a significant duplication of costs, as they will likely have to report bilaterally to several correspondent banks about specific customers.
- As many customers operate through a variety of different entities, a correspondent bank seeking information on a particular customer will get only a partial view of the customer's business profile (as information on payments made by the customer will be limited to the customer's activities with the respondent bank providing the information).

The problems above create an environment with considerable inefficiencies and uncertainty. Moreover, it seems that the biggest problem in this respect is the uncertainty of the banks involved in correspondent banking on what exactly is expected by the relevant authorities in order to fully comply with the current regulatory framework. In order to improve the situation and to provide more clarity, the competent international bodies are working extensively on this issue. In particular, the FATF (the international standard setter in the field of AML/CFT measures), in its statement on de-risking cited above (see Box 1), has committed to continue a number of existing activities and projects providing information and guidance to inform risk-based decision-making, including work on the risk-based approach for banks, the risk-based approach for money or value transfer services, best practices on combating the abuse of non-profit organizations and effective supervision and enforcement. Additionally, the BCBS through its AML/CFT Expert Group has developed guidance on compliance with the FATF recommendations from a supervisory point of view. It might be appropriate to encourage current work by the FATF and the BCBS to increase clarity in this area, given that some of the factors that are lessening the attractiveness of the correspondent banking business relate to the uncertainties around due diligence vis-à-vis the respondent banks' customers, and that the BCBS is developing the relevant FATF recommendations from a supervisory point of view.

In parallel to the ongoing work of the FATF and other relevant bodies, several technical measures might be considered, including some already being implemented in certain jurisdictions. These could include:

- More widespread use of the LEI to unambiguously identify corporate customers (see Section 3.3).
- Banks could include in their contracts with direct customers for cross-border payment services the option of forwarding relevant information to correspondent/intermediary banks. If

[20] Eg the OFAC (Office of Foreign Assets Control) list in the United States, the, EU sanctions list, the Consolidated United Nations Security Council Sanctions List and the FATF list of high-risk and non-cooperative jurisdictions.

authorised by the direct customers and if permitted by data privacy rules, this might facilitate information-sharing between banks, and hence faster investigations and payments processing.

- An initiative worth mentioning in this area is the development of centralised databases for AML/CFT purposes, in which banks would provide information on the identities, business and transactions of their customers active in cross-border payment services. These could help reduce duplicated reporting, as respondent banks would then send such information only to the database, where it could be accessed by all correspondent banks and authorities with a legitimate interest. Centralised databases could also provide correspondent banks with updated and better information, as the transactions related to an individual customer reported by several respondent banks could be aggregated, creating a more comprehensive customer business profile. The management of the highly confidential information stored in such a database might require the support of a public authority, which could also increase the confidence of correspondent banks and their authorities in the reliability of the information. The creation of an information-sharing mechanism for centralising and sharing due diligence information might be an adequate solution for jurisdictions where banks are facing difficulties in opening or maintaining correspondent banking services with other jurisdictions. An example of such a database, in an early stage of development, is the one under development in Mexico to provide information to foreign correspondent banks and improve transaction flows (see Box 4 for details).

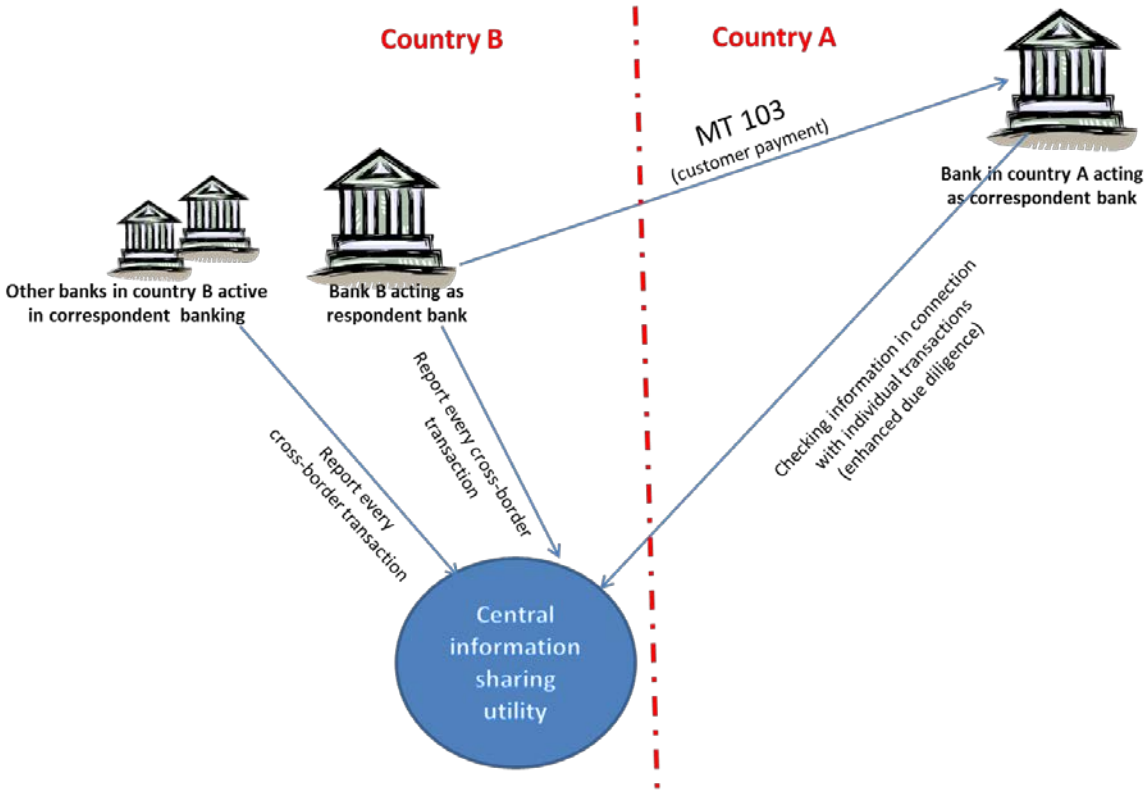
Box 4

Mexican initiative on information-sharing

A centralised database is currently under construction into which Mexican banks will be required to report all cross-border transactions. Banks will also be able to report information on their customers. Thus, the centralised database will consist of two main components: (i) a transactional component with aggregated information of cross-border transactions initiated by customers and (ii) a customer due diligence component with information on each individual customer. The level of information required for each customer will depend on the aggregated number and value of its transactions.

Domestic and foreign authorities could query the database to identify originators and obtain some aggregated data on their transactions. Correspondent banks would thus have access to information about the respondent bank's customers for which they have processed transactions or from which they have received requests to process transactions. Originators would be required to agree to share information.

Domestic authorities would be involved in the regulation and oversight of the database, which would include requirements on information verification to make the database useful for correspondent banks and their authorities. The figure below shows how such central utility might be used.



There are initiatives with certain similarities but also with significant differences in relation to the scope and level of detail of the information stored. In the United States, for example, Section 314(b) of the USA Patriot Act is a voluntary programme that provides financial institutions with the ability to share information with one another, under a safe harbour that offers protections from liability, in order to better identify and report potential money laundering or terrorist activities. This programme is, however, limited to domestic entities and does not contemplate cross-border sharing of information. In

other jurisdictions, such as Turkey, data privacy laws seem to be an unsurmountable obstacle for the implementation of similar initiatives. Within the EU, different laws and the implementation of the 1995 Data Protection Directive have led to different data protection levels. Also in the EU, the Fourth Anti-Money Laundering Directive (AMLD4) has been adopted with the aim to strengthen the EU AML framework, in line with the recently reshaped international AML standards. The directive will for the first time oblige EU member states to keep central registers of information on the ultimate beneficial owners of corporate and other legal entities, as well as trusts. The central registers will be accessible to the authorities and their financial intelligence units (without restriction), to "obliged entities" (such as banks conducting customer due diligence), and also to the public in the case of "legitimate interest". Member states will have two years to transpose the anti-money laundering directive into their national law.

Information-sharing mechanisms could increase the efficiency of procedures and may increase confidence by correspondent banks on the availability of information, reducing the cost of "KYCC" due diligence processes. They face, however, several obstacles and limitations:

- Information-sharing might help to reduce costs but it needs to be kept in mind that correspondent banks always remain responsible for performing adequate due diligence. Information-sharing mechanisms do not alter these basic responsibilities.
- The most important obstacle is compliance with data protection and data privacy laws and regulations. As mentioned above, the communication of transaction or customer information to an information-sharing database might not be allowed in many jurisdictions under various regulations for data protection or for certain persons or entities according to data privacy laws.
- These databases may or may not include information on suspicious transactions. Its potential inclusion is intended to help banks differentiate between customers, ultimately benefiting the innocent. However, false positives (eg due to identical names), available to banks on a mass scale globally, may mistakenly link innocent customers to illicit or undesirable activity. This may result in certain customers or institutions being broadly denied services due to the shared information/shared concern. This, in turn, could result in limited possibilities to conduct payment services even for entirely innocent customers and for the respondent bank and could eventually lead to completely losing their correspondent relationships.
- The concentration of confidential information in a single repository requires that operational risks be adequately managed to address hacking threats that could lead to leakages of information (that could cause serious reputational and legal problems).
- Furthermore, the setup of such databases might be quite costly.

In conclusion, compliance with "KYCC" due diligence expectations is a complex issue. Obvious measures for improvement are difficult to identify from a technical perspective and these activities cannot be easily outsourced, because responsibility for due diligence always remains with the banks.

Further FATF work in close cooperation with other relevant authorities in this field may help to diminish the uncertainties that correspondent banks are currently facing. At the same time, some technical improvements (eg information-sharing mechanisms) could support more efficient processes for information exchange – provided that data privacy laws permit this.[21]

Recommendation: 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

[21] Although data privacy standards are beyond the FATF or BCBS remit, these bodies could explore, possibly in cooperation with other authorities, the interaction and consistency between AML/CFT requirements and data privacy issues.

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.

3.5 Payment messages

3.5.1 General considerations

As described in Section 2.1, correspondent banking transactions are channelled and settled through a chain of bilateral relationships between respondent and correspondent banks (sometimes also involving payment systems[22]). This section focuses on the payment message flows and formats. It describes the payment processes commonly used in correspondent banking, discusses some of the advantages and drawbacks of the different messaging methods, and identifies potential issues that might be considered by the industry and authorities with a view to facilitating cross-border correspondent banking services.

In general, SWIFT message formats are non-proprietary and can also be used over other networks. However, the network used in the overwhelming majority of correspondent banking relationships is the SWIFT network. Accordingly, the description below focuses on SWIFT message formats and assumes that respondent and correspondent banks, as well as any intermediary institution, have access to the SWIFT network and use its SWIFT message formats for correspondent banking activities.

3.5.2 Message flows

A simple cross-border correspondent transaction would entail a payment from a customer of the respondent bank to a customer of the correspondent bank in a different jurisdiction. These customers can be individuals, small or medium-sized entities (SMEs), corporates, public sector agencies or other financial institutions. In its simplest form, the respondent has a direct bilateral account relationship with the correspondent, and thus the payment information and the settlement instruction can travel in a single message. The SWIFT standard for these customer payment messages is the MT 103.[23,24] Figure 2 below provides a generic overview of a simple cross-border transaction.

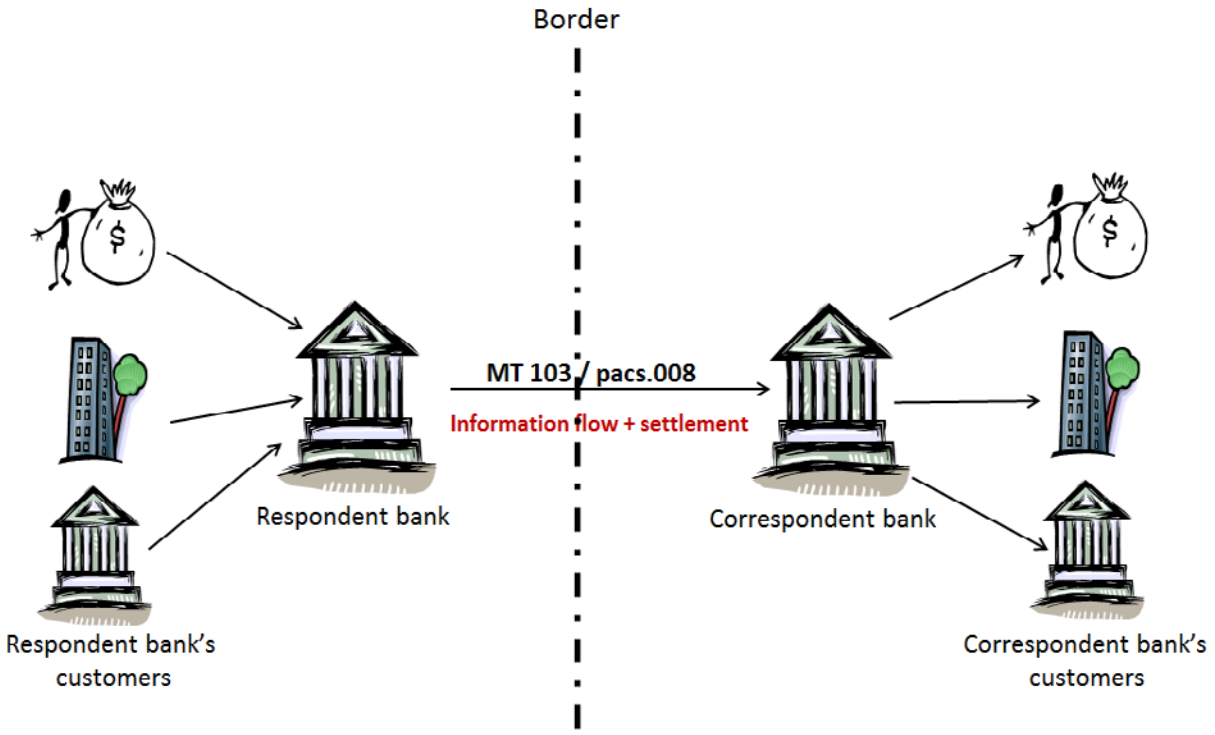
[22] In general, the working group focused on cross-border payments. However, the complete payment chain of cross-border correspondent banking payments may also include transfers between institutions in a single jurisdiction, which usually take place through payment systems. Payment systems may also be used in some cases to transfer payments through different jurisdictions.

[23] For examples of MT 103, see: www.swift.com.

[24] In addition to the MT message types, there are equivalent MX message types. The MX equivalent for the MT 103 is the pacs.008 (credit transfer message). However, MT message formats are normally used in correspondent banking.

Figure 2

A simple cross-border correspondent transaction



However, in many cases the respondent bank originating the payment does not have a direct bilateral account relationship with the correspondent bank receiving the payment. In these cases, it is necessary to find a chain of one or more intermediary banks to transmit the funds from the respondent bank to the correspondent bank. These intermediary institutions also provide correspondent banking services to the other banks in the chain. These types of relationships are very common in cross-border correspondent banking. Payment chains can be quite long, involving banks in more than two jurisdictions.

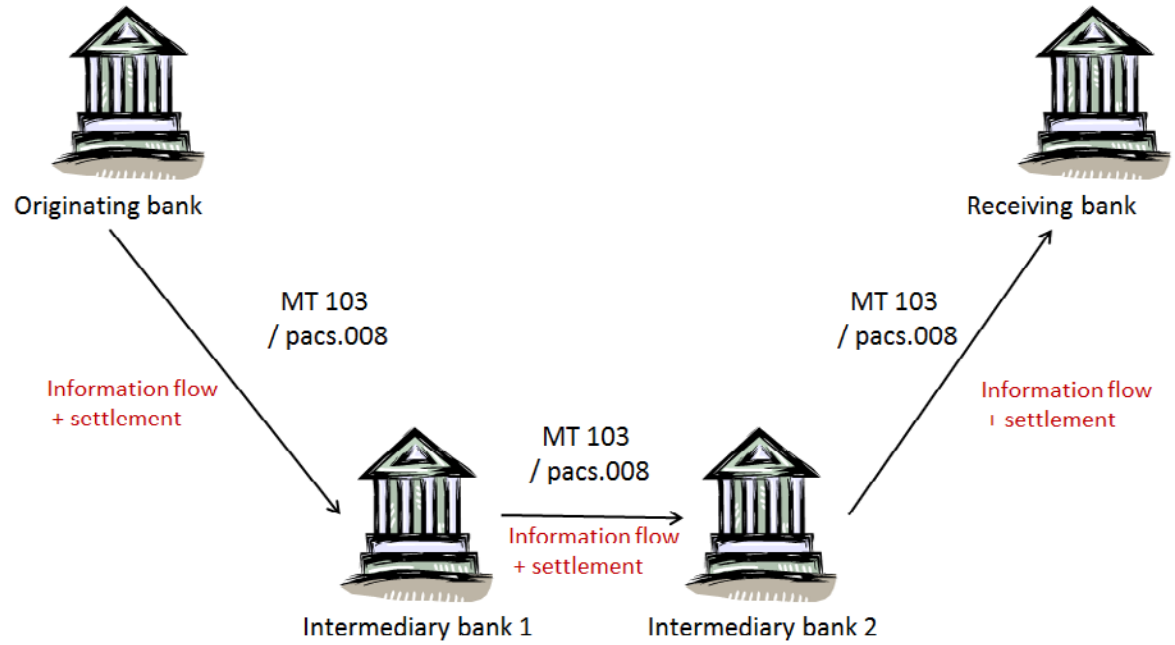
There are two basic ways of channelling a correspondent banking transaction through the SWIFT network when the originating institution has no direct bilateral account relationship with the receiving bank: the **serial method** and the **cover method**.

- The **serial method** involves sending an MT 103 (or equivalent) from the originating bank to the receiving bank through one or more intermediaries. This method is just an extended concatenation of simple transactions between respondent and correspondent banks (as outlined above), each pair having a direct account relationship. The payment information and the settlement instruction travel together in the MT 103 message and there exists a direct account relationship[25] between each connected pair of banks in the payment chain (see Figure 3 below).

[25] The usage of payment systems is not considered for reasons of simplicity.

Figure 3

A correspondent transaction using the serial method



- The **cover method** decouples the settlement from the payment information. The MT 103 with the payment information is sent directly through the SWIFT network from the originating bank to the receiving bank, whereas the settlement instruction (the cover payment) is sent via intermediary banks through the path of direct correspondent banking relationships.

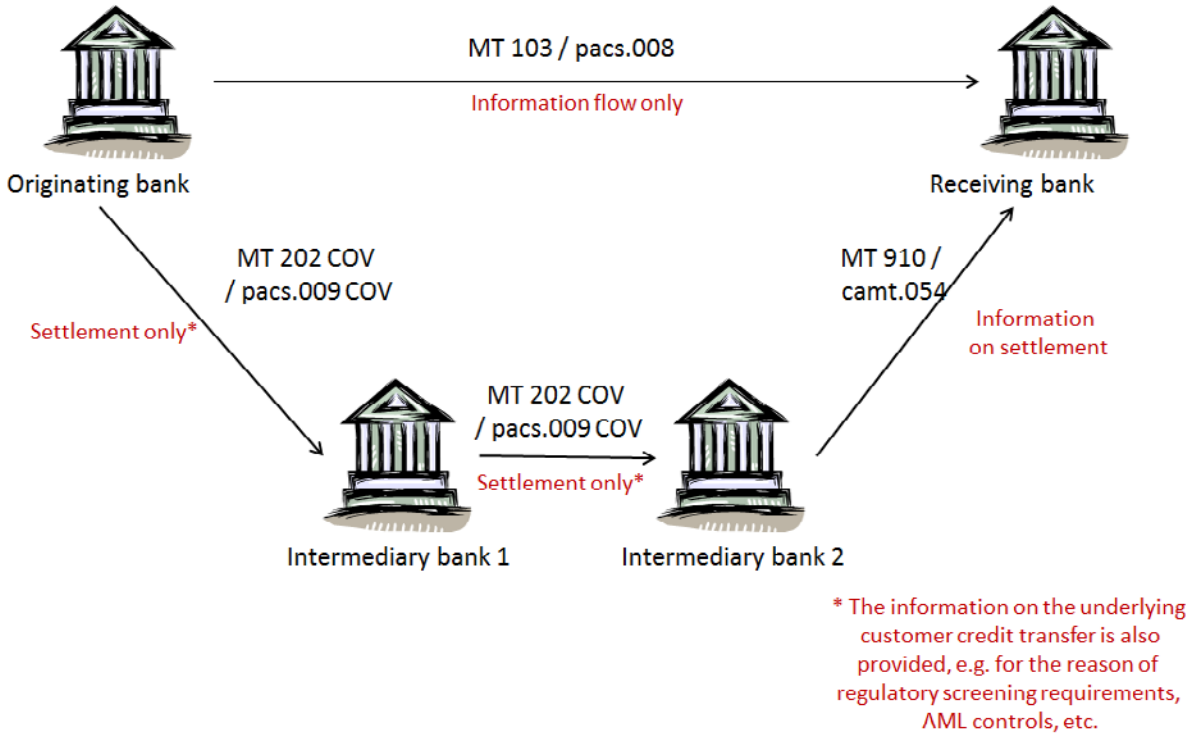
  Traditionally, cover payments were made using the MT 202 format (the standard SWIFT interbank transfer message). This message, however, was not designed to carry detailed information on the ordering customer and final beneficiary of the transfer (ie the customers of the first and last banks in the chain, see Figure 4 below). As a result, intermediary banks were not able to screen these transactions properly according to AML/CFT and sanctions requirements, and they could even remain unaware that the MT 202 interbank transfer was related to a commercial correspondent banking payment.

  To tackle this problem, a common effort of SWIFT, banks involved in correspondent banking activities and authorities took place to devise a solution that would allow all banks in the payment chain to conduct proper screening of correspondent banking transactions. These efforts resulted in the MT 202 COV, a new message standard for interbank transfers related to correspondent banking cover payments that was implemented in the 2009 standards release. The main advantages of the MT 202 COV are that (i) it allows maintaining the principle of making cover payments by using interbank transfer messages (which was the prevalent approach at that time), and (ii) it is designed to carry all the necessary details about the identities of the ordering customer and the final beneficiary as well as other information on the payment that are included in the underlying MT 103 message. Therefore, if the code "COV" is used in field 119 of the message user header, it is mandatory to fill in an additional sequence in the message to include a copy of selected fields from the underlying customer credit transfer

(ie the MT 103). The adoption of the MT 202 COV has led to a ban on the use of plain MT 202 messages in correspondent banking whenever an underlying customer transaction is involved.[26]

Figure 4

A correspondent transaction using the cover method



Both methods can be used in full compliance with AML/CFT as well as relevant regulatory requirements. When all data fields are correctly populated, both the serial method and the cover method provide all banks involved with the necessary information about the payment, allowing them to conduct an adequate screening of the transaction and fulfil all regulatory requirements.

Nevertheless, there are some differences between the two methods which need to be examined more closely in order to decide which method might be more advantageous from a safety and efficiency perspective:

- Ensuring the availability of all necessary information within the payment message.

When using the MT 202 COV, the originating bank must correctly flag the MT 202 message as a cover message in order to ensure that all information relevant for AML/CFT procedures is provided. If the originating bank does not provide this information – perhaps as a result of technical problems or even with fraudulent intent – the other banks in the payment chain will not receive all relevant information. Moreover, since an MT 202 payment without the cover indicator is a simple interbank payment, the

[26] Note that the introduction of the MT 202 COV has not led to the abandonment of the MT 202 interbank transfer message, which remains appropriate for pure interbank transactions (ie those unrelated to commercial correspondent banking services). Details of MT 202 as well as MT 202 COV usage can be found in the SWIFT User Handbook.

intermediary banks will accept the MT 202 and be unaware that relevant information is missing. Therefore, the risk exists that a bank could unknowingly accept a message without complete information. In this case, the intermediary bank might not be able to fulfil its regulatory obligations.

When using the MT 103 in the serial method, the risk that a bank is unaware of missing information does not arise because all relevant information is included in the MT 103. If some information is missing, this will be obvious to every involved bank as not all fields in the message will be completed with the required information.

- Fees and costs

By current market practice, banks do not deduct fees from MT 202/MT 202 COV messages. Thus, for payments sent with the MT 202 COV method, banks involved in the payment chain (eg as intermediaries) do not deduct additional fees. With regard to MT 103, according to the current market practice, a fee is typically deducted from the payment amount by each intermediary bank so that, in such cases, the beneficiary does not receive the full amount of the original payment order.

Besides the fees charged, other cost elements also need to be considered when assessing the costs of each payment method. For example, when the cover method is used, two SWIFT messages need to be sent by the originating bank and two messages need to be processed by the receiving bank. It is worth noting here that most of the costs involved in correspondent banking arise not from the actual payments processing but from compliance and IT work on system modifications.

As comprehensive cost calculations can only be done at the level of individual banks, it is not possible to say a priori which payment method is cheaper. Some banks consulted for this report have suggested that the differences in costs between the two methods have been exaggerated.

- Message flow

In general, the cover method is considered to be faster. Nevertheless, when using the cover method, two separate flows exist. On the one hand, this means that the receiving bank is aware that it will receive funds and, should the bank not receive the expected funds via MT 202 COV, it can then investigate. On the other hand, depending on the commercial policies of a receiving bank, this knowledge either allows an early credit on the customer account or it might put the bank under pressure – for competitive reasons – to credit the sum to the account of its customer before it actually receives the funds (eg in the case of large corporates). This might be especially critical in cases where the beneficiary bank has received the MT 103 but the MT 202 COV is stopped or rejected by one of the banks involved in the payment chain due to compliance concerns. Therefore, banks need to ensure that appropriate unwinding procedures are in place to reverse a credit on the account should the need arise. Moreover, as mentioned above, the receiving bank always needs to "match" both message flows.

- Payment advice

In the case of the serial MT 103, the information and the settlement reach the receiving bank at the same time, eliminating any lag between the information and settlement. It needs to be acknowledged that, in this case, the receiving bank will not be aware that a payment is coming until the MT 103 is processed by all intermediary banks. This potential drawback can be solved – if need be – through alternative means.[27]

[27] For example, SWIFT FINInform, a service within the SWIFT network, allows a copy of a message to be sent to specific third parties following predefined rules. If need be, this can be used to send a copy of an MT 103 that will be processed following the serial method to the receiving bank. This copy ensures the accuracy of the information and it would preannounce the reception of a payment in the same way as the MT 103 does in the cover method. When using the SWIFT FINInform service, the receiving bank needs to ensure that adequate procedures are in place in order to avoid an erroneous double processing of the MT 103.

While acknowledging the advantages and drawbacks of both methods, and in particular that the implementation of the MT 202 COV in 2009 was the result of a common effort accompanied by a long consultation process, it might still be worthwhile to restart a discussion on the different methods. The increasing importance of AML/CFT screening procedures in correspondent banking might be tilting the balance towards methods perceived to be safer (ie the serial MT 103) for some intermediary banks. According to information received by several working group members, some intermediary banks require that respondent banks located in some jurisdictions use only the serial method for correspondent banking transactions. But other members are unaware of this trend.

Any debate on this issue needs to proceed cautiously, as the current methods reflect a long history of market practice and some difficult compromises between the various stakeholders. Any change would have to be preceded by an adequate consultation process and any recommendation or mandatory change would necessarily take into account potential costs related to the adaptation of the messaging network and banks' internal systems and also unintended consequences (eg, abandoning the MT 202 COV in favour of the serial method might cause some banks to start misusing the MT 202 for cover payments in correspondent banking, a practice that could be very difficult to detect for intermediary banks).

Recommendation: 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.

3.5.3 Usage of the LEI in payment messages

Currently, payment messages include neither a dedicated code nor a dedicated line for the LEI. The LEI can be used in free format fields, but no validations apply in order to check whether an LEI is included and whether it is syntactically correct. However, in the long term, and as payment messages evolve, a discussion on the development of such dedicated codes or data items could take place when changes in payment message formats[28] would need to be discussed anyway, as the LEI would promote the unambiguous identification of parties to a transaction.[29]

Should the use of LEIs become widespread or even compulsory for banks as well as for corporate customers (see Section 3.3 for a detailed discussion of LEI usage), the potential implications for payment messages would need to be analysed in detail. Various options for including the LEI in the payment message exist: (i) development of specific data fields and their inclusion in message formats used for correspondent banking transactions, such as the MT 103 or MT 202 COV (and equivalents) or (ii) the use of a dedicated code for the LEI within the payment message or (iii) the development of a market practice in which the LEI can be included in an existing field of the payment message. Moreover, if the LEI were included, it would need to be clarified with the relevant authorities whether the regulatory framework provides clear guidance on how to deal with any contradictions between the LEI and other party references (eg an account number) included in the payment message.

[28] This might be the case, for example, when at some point in the future ISO20022 messages are considered for use in correspondent banking, as such a change would imply changes to bank IT systems in any case. In the area of securities messages, however, discussions are already ongoing in order to allow the LEI to be used as a party identifier across ISO 15022 category 5 messages.

[29] As mentioned in Section 3.3, it needs to be kept in mind that no LEI for individuals exists.

This analysis would need to be undertaken in close cooperation with the banks involved in the correspondent banking business in order to avoid any unintended consequences for costs and processing.

All in all, it seems premature to promote a requirement of including the LEI in payment messages for the time being (due to its limitations and the high transition costs). Therefore, no recommendation on this point is made here.

4. Conclusions

Correspondent banking services are an essential component of the global payment system, especially for cross-border transactions. There seems to be a variety of reasons for the general reduction of correspondent banking relationships that is being detected by many stakeholders, but compliance with AML/CFT regulations, an increased perception of risk and some uncertainties on the potential impact of non-compliance are often mentioned by correspondent banks as reasons for this reduction.

The impact of this trend is uneven across jurisdictions and banks. Some correspondent banks specialise in the for-profit provision of correspondent banking services, and thus focus on respondent banks with business volumes that justify the rising costs. Others apparently maintain existing correspondent banking services only as far as these services support the cross-selling of other products. Some relationships are maintained or terminated according to the perceived degree of risk in the respondent bank's jurisdiction. As a result, some respondent banks might risk being cut off from the international payment networks. This trend implies a risk that cross-border payment systems will become fragmented, reducing the options available for these transactions.

The working group limited its analysis to several technical measures that could help to improve efficiency of procedures while reducing compliance costs and perceived uncertainties, without altering the applicable rules and the basic channels for correspondent banking between correspondent and respondent banks. The potential measures were translated into four technical recommendations.

The working group believes that its recommendations might alleviate some of the costs and concerns connected with correspondent banking activities. However, the members are aware and would like to stress that, in isolation, these technical measures will not resolve all such issues. The working group acknowledges that the issues surrounding the withdrawal from correspondent banking are very complex and that costs related to AML/CFT compliance are only one of the elements that have to be considered in order to understand recent trends. Those include business considerations as well as economies of scope and scale issues. Limiting information challenges through the use of enhanced technical tools will only address part of AML/CFT compliance costs but does not resolve issues such as uncertainty about how far customer due diligence should go. In particular, the proposed technical measures will not immediately help the banks without access to correspondent banking services to gain such access.

The measures which could facilitate the provision of correspondent banking services analysed in this report relate to: (i) Know-your-customer (KYC) utilities, (ii) increased use of the LEI, (iii) information-sharing mechanisms, and (iv) improvements in payment messages.

As a next step before any potential implementation, these measures should be subject to a formal consultation and further analysed by all relevant stakeholders in order to gauge the potential impact of each measure and to avoid unintended consequences.

Annex 1 - References

Basel Committee on Banking Supervision AML/CFT Expert Group (2014): *Sound management of risks related to money laundering and financing of terrorism*, http://www.bis.org/publ/bcbs275.pdf.

Committee on Payments and Market Infrastructures (2015): *A glossary of terms used in payments and settlement systems*, http://www.bis.org/cpmi/publ/d00b.htm?m=3%7C16%7C266

European Central Bank (2015): *Ninth survey on correspondent banking in euro*, 2014, http://www.ecb.europa.eu/pub/pdf/other/surveycorrespondentbankingineuro201502.en.pdf.

FATF (2012): *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, www.fatf-gafi.org/recommendations.

FATF (2014): *Risk-Based Approach for the Banking Sector*, http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf.

FATF (2015): *FATF clarifies risk-based approach: case-by-case, not wholesale de-risking*, http://www.fatf-gafi.org/topics/fatfgeneral/documents/rba-and-de-risking.html.

FATF (2015): *Dialogue with the Private Sector - FATF Private Sector Consultative Forum Meeting*, Brussels, 26–27 March 2015, http://www.fatf-gafi.org/documents/documents/private-sector-forum-march-2015.html.

FATF (2015): Drivers for "de-risking" go beyond anti-money laundering / terrorist financing, http://www.fatf-gafi.org/topics/fatfrecommendations/documents/derisking-goes-beyond-amlcft.html.

The Wolfsberg Group (2014): *Wolfsberg Correspondent Banking Principles*, http://www.wolfsberg-principles.com/pdf/home/Wolfsberg-Correspondent-Banking-Principles-2014.pdf.

Various contributors (eg BBA and Wolfsberg Group) (2014): *De-risking; global impact and unintended consequences for exclusion and stability*; paper prepared for use by the October 2014 FATF Plenary and associated working groups.

Annex 2 – Glossary

Glossary	
Terms	Definition
Beneficiary	Beneficiary refers to the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer.[30]
Beneficiary financial institution	Beneficiary financial institution refers to the financial institution which receives the wire transfer from the ordering financial institution directly or through an intermediary financial institution and makes the funds available to the beneficiary.[31]
BIC	BIC is the international ISO standard ISO 9362:2014. This standard specifies the elements and structure of a universal identifier code, the business identifier code (BIC), for financial and non-financial institutions, for which such an international identifier is required to facilitate automated processing of information for financial services. The BIC is used for addressing messages, routing business transactions and identifying business parties. SWIFT in its role of ISO registration authority issues BICs to financial and non-financial institutions. The BIC is used in financial transactions, client and counterparty databases, compliance documents and many others.[32]
Correspondent banking	Correspondent banking is an arrangement under which one bank (correspondent) holds deposits owned by other banks (respondents) and provides payment and other services to those respondent banks. Such arrangements may also be known as agency relationships in some domestic contexts. In international banking, balances held for a foreign respondent bank may be used to settle foreign exchange transactions. Reciprocal correspondent banking relationships may involve the use of so-called nostro and vostro accounts to settle foreign exchange transactions.[33] *Note: For the purpose of this report correspondent banking is considered as the provision of cross-border payment services only.*

30 See "The FATF Recommendations", Glossary, February 2012.

31 See "The FATF Recommendations", Glossary, February 2012.

32 See www.swift.com.

33 See BIS, CPSS Glossary, March 2003.

Cover Payment	Cover Payment refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions[34]. An MT202 COV shall be used.[35]
Customer due diligence (CDD)	CDD measures to be taken are as follows: a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information. b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer. c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship. d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds. Financial institutions should be required to apply each of the CDD measures under (a) to (d) above, but should determine the extent of such measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1.[36]
Intermediary financial institution	Intermediary financial institution refers to a financial institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.[37]
Legal Entity Identifier (LEI)	The Legal Entity Identifier (LEI) is a 20-digit, alpha-numeric code, to uniquely identify legally distinct entities that engage in financial transactions.[38]

[34] See "The FATF Recommendations", Glossary, February 2012.

[35] See www.swift.com.

[36] See "The FATF Recommendations", February 2012.

[37] See "The FATF Recommendations", Glossary, February 2012.

[38] See www.leiroc.org.

MT 103	The MT 103 allows the exchange of single customer credit transfers. The MT 103 can be straight through processable if the message is properly formatted according to pre-agreed bilateral/multilateral rules.[39]
MT 103 STP	The MT 103 STP is a general use message, ie, no registration in a message user group is necessary to send and receive this message. It allows the exchange of single customer credit transfers using a restricted set of fields and format options of the core MT 103 to make it straight through processable. The MT 103 STP is a compatible subset of the core MT 103 that is documented separately. The differences with the core MT 103 are inter alia: • appropriate MT 103 STP format validation is triggered by the code STP in the validation flag field 119 ({3:{119: STP}}) of the user header of the message (block 3); • fields 52, 54, 55, 56 and 57 may only be used with letter option A; • field 53 may only be used with letter options A and B; and field 51A is not used in MT 103 STP. This message may only be used on the SWIFTNet FIN network since it requires special validation.[40]
MT 202	The MT 202 is a general financial institution transfer. This message is sent by or on behalf of the ordering institution directly, or through correspondent(s), to the financial institution of the beneficiary institution. It is used to order the movement of funds to the beneficiary institution. This message may also be sent to a financial institution servicing multiple accounts for the sender to transfer funds between these accounts. In addition it can be sent to a financial institution to debit an account of the sender serviced by the receiver and to credit an account, owned by the sender at an institution specified in field 57a. This message must not be used to order the movement of funds related to an underlying customer credit transfer that was sent with the cover method. For these payments the MT 202 COV or MT 205 COV must be used.[41]

[39] See www.swift.com.

[40] See www.swift.com.

[41] See https://www2.swift.com/uhbonline/books/public/en_uk/us2m_20140725/index.htm?subpage=ahg.htm.

MT 202 COV	This message is sent by or on behalf of the ordering institution directly, or through correspondent(s), to the financial institution of the beneficiary institution. It must only be used to order the movement of funds related to an underlying customer credit transfer that was sent with the cover method. The message contains a mandatory sequence to include information on an underlying customer credit transfer. Guidelines for the use of the message have been published by the Payments Market Practice Group (PMPG). [42] The MT 202 COV must not be used for any other interbank transfer. For these transfers the MT 202 must be used.[43]
Ordering financial institution	Ordering financial institution refers to the financial institution which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.[44]
Originator	Originator refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.[45]
Serial payment	Serial payment refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (eg correspondent banks).[46]
Upstream bank	Upstream bank is a bank that provides correspondent banking services to another bank. Therefore, an upstream bank has to ensure that it fulfils all requirements with respect to customer due diligence.
Wire transfer	Wire transfer refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.[47]

42 See www.pmpg.info.

43 See https://www2.swift.com/uhbonline/books/public/en_uk/us2m_20140725/index.htm?subpage=ahg.htm.

44 See "The FATF Recommendations", Glossary, February 2012.

45 See "The FATF Recommendations", Glossary, February 2012.

46 See "The FATF Recommendations", Glossary, February 2012.

47 See "The FATF Recommendations", Glossary, February 2012.

Annex 3 - Members of the CPMI Working Group on Correspondent Banking

Chairman	Jochen Metzger Deutsche Bundesbank
Members	
National Bank of Belgium	Pierre Gourdin
European Central Bank	Dieter Reichwein
Bank of France	Adrien Delcroix
Deutsche Bundesbank	Roland Neuschwander
Bank of Japan	Fusako Watanabe
Bank of Korea	Jinman Choi
Bank of Mexico	Miguel Díaz
Netherlands Bank	Jurgen Spaanderman
Sveriges Riksbank	Felice Marlor
Swiss National Bank	Martin Blättler
Central Bank of the Republic of Turkey	Kenan Koc
Bank of England	Justin Jakobs
Board of Governors of the Federal Reserve System	Jeffrey Marquardt Koko Ives
CPMI Secretariat	Carlos Conesa Yuuki Shimizu

Significant contributions were also made by Tim Masela (South African Reserve Bank), Lee Davis (Board of Governors of the Federal Reserve System), Anja Hartmann (Deutsche Bundesbank) and Ralf Schmidt (Deutsche Bundesbank).