Guidance on Correspondent Banking Services

هيئة تنظيم مركز قطر للمال

QATAR FINANCIAL CENTRE
REGULATORY AUTHORITY

Confidential – not for further distribution.

TABLE OF CONTENTS

Version control:

Guidance on the Risk-Based Approach
V3.0
May 2018

GLOSSARY OF TERMS

AML/CFT	State of Qatar AML/CFT Law
BCBS	Basel Committee on Banking Supervision
BO	Beneficial Owner
CDD	Customer Due Diligence
CBR	Correspondent Banking relationship
DNFBP	Designated Non-Financial Business or Profession
FATF	Financial Action Task Force
FI	Financial Institution
KYC	Know Your Customer
ML	Money Laundering
MTO	Money Transfer Operator
PEP	Politically Exposed Person
TF	Terrorist Financing
UBO	Ultimate Beneficial Owner

1. PURPOSE

1.1 The term "Firm(s)" is used to denote FIs and DNFBPs.

1.2 The purpose of this document is to provide Firms with guidance on general principles and best practice in relation to correspondent banking services. This guidance excludes customer due diligence (CDD) requirements related to wire transfer services, transparency in cover payment messages, and money or value transfer services, as detailed guidance on these topics have separately been published by FATF and BCBS.

1.3 Pressure on global banks to comply with stringent AML and CFT regulations has caused certain institutions to consider 'de-risking', or exiting relationships to limit risk exposure rather than managing risk, particularly in relation to providing correspondent banking services. This has had the unintended consequence of depriving many smaller respondent banks in effectively engaging with banks that have traditionally provided correspondent services. There have been instances of global banks closing down relationships with many of their respondent banks, especially in emerging economies, partly for commercial reasons but mainly because these smaller banks cannot always meet today's higher standards for combating financial crime.

1.4 FATF has been discussing this problem with banks since the middle of 2015 and in October 2016 clarified the expectations regarding the AML/CFT standards on CDD:

- ✓ FATF's AML and CFT Recommendations "do not require correspondent financial institutions to conduct CDD on each individual customer of their respondent institutions' customers". In other words, while they must apply the principle of KYC, this does not extend to knowing-your-customer's-customer (KYCC).
- ✓ Not all correspondent banking relationships carry the same level of money laundering or terrorist financing risk, so CDD has to be commensurate with the risks identified.

1.5 This guidance does not replace the State of Qatar AM/CFT Law or other applicable AML/CFT laws, regulations and rules in force in the State of QatarIt is not legal advice, and is not intended to be a detailed analysis of Qatar's legislative requirements.

1.6 In all situations, Firms remain responsible for ensuring that they have appropriate policies, procedures, systems, and controls in place to achieve compliance with all relevant AML/CFT laws, regulations and rules in force in the State of Qatar. Firms will find it beneficial to consider this guidance alongside other guidance papers, in particular those on CDD and the Risk-Based Approach.

2. OVERVIEW OF CORRESPONDENT BANKING SERVICES

2.1 Correspondent banking is the provision of banking services by a bank (the correspondent) to another bank (the respondent). Correspondent banking services enable respondent banks to conduct business and provide services that they cannot offer otherwise, typically owing to the lack of an international presence and direct access to cross-border payment systems. The provision of

correspondent banking services is also a critical factor in facilitating international trade.

2.2 A correspondent banking arrangement involves one bank (the correspondent) providing a deposit account or other liability account, and related services, to another bank (the respondent), often including its affiliates. The arrangement requires the exchange of messages between banks to settle transactions by crediting and debiting accounts. These messages could be associated with payments, trade finance, foreign exchange, or securities transactions (See Annexure 2).

2.3 Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services[1].

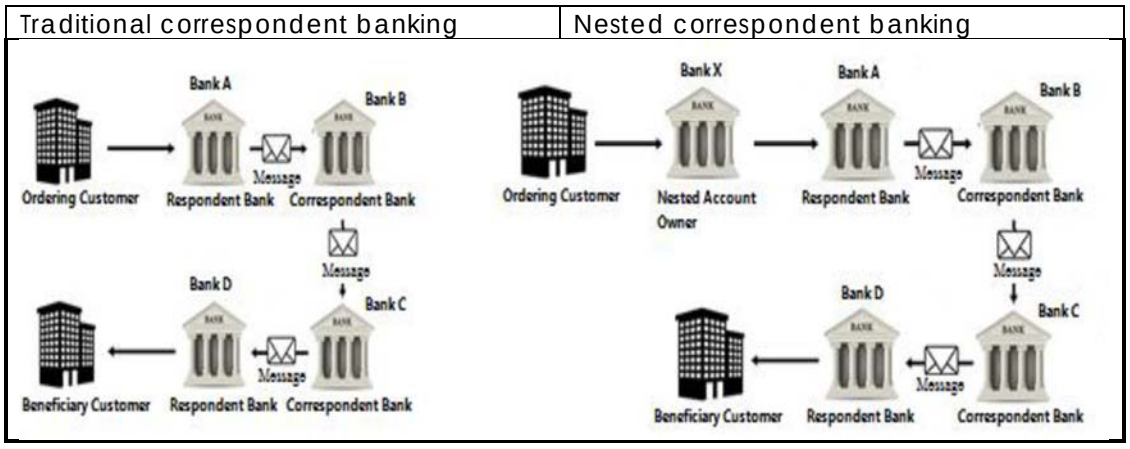
2.4 Correspondent banking services are provided in three main forms (Figure 1).

1) The most traditional form of correspondent banking involves a respondent bank entering into an agreement with a correspondent bank to execute payments on its own behalf and on behalf of its direct customers.

2) Nested correspondent banking refers to the use of a Correspondent Banking relationship ("CBR") by a respondent bank's intermediate customers (e.g., banks and financial institutions), which could then use the relationships for their own customers.

3) Payable-through accounts are similar to nested correspondent banking, but in the case of these accounts, the respondent bank allows its intermediate customers to access the correspondent account directly to conduct business on their own behalf.

Figure1: Examples of correspondent banking payment transactions



[1] Glossary in the FATF 40 Recommendations http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

2.5 Correspondent banking relationships also support payment solutions performed by other financial institutions, including money transfer operators (MTOs). With respect to remittance flows, CBRs support the channelling of small payments that have generally been aggregated by small financial intermediators. These institutions collect small amounts of remittances and use CBRs or their relationships with respondent banks to send the aggregate amounts to the account of their counterparts, which will subsequently redistribute the remittances to the beneficiaries.

2.6 A correspondent relationship is characterised by its on-going, repetitive nature and does not generally exist in the context of one-off transactions. Although this guidance addresses the relationships maintained with other banks, institutions may decide to extend this to all the relationships which they maintain for non-bank financial institutions. These principles may also be applied to SWIFT Relationship Management Application (RMA) relationships in part, or in totality, using a risk-based approach.

2.7 Correspondent banks that execute and/or process transactions for customers of respondent banks generally do not have direct business relationships with these customers, who may be individuals, corporations or financial services firms, established in jurisdictions other than that of the correspondent bank. Thus the customers of the correspondent bank are the respondent banks. Correspondent banks are therefore required to conduct appropriate due diligence on the respondent banks, and are not required to do so on the respondent banks' customers.

2.8 Because of the structure of this activity and the limited information available regarding the nature or purpose of the underlying transactions, correspondent banks may be exposed to ML/TF risks.

3. IDENTIFYING ML/TF RISKS IN CORRESPONDENT BANKING

3.1 Due diligence on the respondent bank

All correspondent banking customers should be subjected to appropriate due diligence that will seek to satisfy an institution that it is comfortable conducting business with a particular customer, given the customer's risk profile and the nature of the business relationship with that customer. It may be appropriate for an institution to consider, but never rely on solely, the fact that the customer operates in a regulated environment which is internationally recognised as adequate in the fight against ML/TF. In such circumstances, an institution may also rely on publicly available information obtained either from the customer or reliable third parties (regulators, exchanges, etc.) to satisfy its due diligence requirements.

Risk indicators that correspondent banks should consider in their risk assessment should include:

1. Inherent risk in the nature of services being provided:
    - The purpose of the services provided to the respondent bank (e.g. foreign exchange services for respondents' proprietary trading, securities trading on

recognised exchanges or payments between a respondent's group within the same jurisdiction may constitute indicators of lower risk);

- Understand how the respondent institution would be offering services available through the correspondent banking relationship to its customers, and assess the nature and level of risk associated with offering arrangements. These could be:
  - By establishing correspondent accounts to which the respondent institution's financial institution customers do not have direct access, but instead transact indirectly through the account via payment instructions delivered to the respondent institution;
  - by establishing nested relationships[2] (i.e. downstream banking); and
  - by establishing payable-through accounts, provided that the correspondent institution identifies risks associated with the relationship and applies enhanced controls to monitor transaction activity that are commensurate with the identified risks.

2. The characteristics of the respondent bank, in particular:

- The respondent bank's major business activities, including target markets and overall types of customers served in key business lines, with particular attention paid to higher-risk customer segments such as PEPs, money service businesses, and non-profit organisations;
- The respondent bank's management and ownership (including the beneficial owners) and whether they represent specific ML/TF risks (e.g. PEPs);
- The respondent bank's AML controls. In practice, such an assessment should involve reviewing the respondent's AML/CFT systems and controls, policies and procedures, including a description of the CDD measures applied by the respondent bank to its customers, and the correspondent bank's ability to obtain information on a particular transaction; and
- Whether any civil, administrative or criminal actions or sanctions, including public reprimands, have been applied by any court or supervisory authority to the respondent bank, when it occurred, the severity, and how the respondent bank addressed the identified shortcomings.

3. The environment in which the respondent bank operates, in particular:

- The jurisdiction in which the respondent bank (and its parent company where the respondent bank is an affiliate) is located;
- The jurisdictions in which subsidiaries and branches of the group may be located, as well as the jurisdictions in which third parties using the correspondent banking relationship may be located; and
- The quality and effectiveness of banking regulation and supervision in the respondent's country (especially AML/CFT laws and regulations) and the respondent's parent company country when the respondent is an affiliate.

The correspondent should have policies, procedures and processes in place to enable it to identify the ultimate user of the account; be satisfied that the respondent institution has conducted sufficient CDD on the customers having direct access to the account of the correspondent institution and has appropriate controls in place to identify and monitor

[2] Nested correspondent banking refers to the use of a bank's correspondent banking relationship by a number of respondent banks through their relationships with the banks' direct respondent bank to conduct transactions and obtain access to other financial services.

the transactions conducted by those customers, and is able to provide in a timely manner relevant individual CDD information upon request to the correspondent institution.

Correspondent institutions, in assessing the risks of the respondent institutions, must ensure that the assessment is sufficiently robust to consider all the relevant risk factors. The assessment must evidence the correspondent institution's understanding of the different levels of inherent risks, the application of appropriate controls to each, ensuring the effective management of these risks. The correspondent institution may apply additional measures that will vary on a case-by-case basis, depending on the level or type of residual risk, including the measures the respondent institution has implemented to mitigate its own ML/TF risks.

3.2 ENHANCED DUE DILIGENCE

Understanding that the business of correspondent banking is high risk by its very nature, the conduct of basic due diligence for correspondents should be more rigorous than it is for other types of accounts. In addition to conducting basic due diligence, each correspondent bank should also apply enhanced due diligence to those respondent banks which present greater risks. The enhanced due diligence process should involve further considerations of higher risk business and associated controls.

1. PEP involvement

   If a PEP appears to have involvement in the respondent bank's operations, then the correspondent bank must ensure that the respondent bank has a wholesome understanding of the person, their role and the appropriateness of that role, their ability to influence the respondent, and the risk they may present to the relationship.

2. Downstream correspondents

   Nested, or downstream, correspondent banking refers to the use of a bank's correspondent relationship by a number of respondent banks and other non-bank financial institutions such as MSBs, through their relationships with the bank's direct respondent bank to conduct transactions and obtain access to other financial services.

   Downstream correspondent banking relationships are an integral and generally legitimate part of correspondent banking. Nesting may be a way for regional banks to help small local banks within the respondent's region obtain access to the international financial system or to facilitate transactions where no direct relationship exists between banks.

   Providing access to third-party foreign financial institutions that are not the customer of the correspondent bank, and so not necessarily known, can conceal financial transparency and increase ML/TF risks. Hence, correspondent banks should require that respondent banks disclose whether accounts include nested relationships as part of account opening and ongoing risk profile reviews. Respondent banks should disclose accurate information regarding the existence of nested relationships.

   Correspondent banks should assess the ML/TF risk associated with customers which are respondent banks with nested relationships on an individual basis, consistent with the risk-based approach. The level of risk may vary depending on the nature of nested foreign financial institutions served by respondent banks, including size and

geographical location, products and services offered, markets and customers served, and the degree of transparency provided by the respondent bank.

In order to assess the ML/TF risks associated with a nested relationship, correspondent banks should understand the purpose of the nested relationship. To this end, they may consider the following factors, among others:

- The number and type of financial institutions a respondent bank serves;
- Whether the banks under the nested relationship are located in the same jurisdiction as the respondent or a different country;
- Whether the jurisdiction of the nested bank and the areas the nested bank serves have adequate AML/CFT policies according to available public information;
- The types of services the respondent offers to nested banks (proprietary only or customer services such as correspondent banking);
- The length of the relationship between the correspondent and respondent banks (e.g. a long-standing relationship which enables the correspondent bank to have a good understanding of the ML/TF risk associated with the relationship versus a new one); and
- The adequacy of the due diligence programme of the respondent bank to evaluate the AML/CFT controls on its nested banks. The due diligence programme should be updated periodically and provided to the correspondent bank at its request.

4. INFORMATION GATHERING

Before entering into a business relationship with a respondent bank, correspondent banks should gather sufficient information to understand the nature of the respondent's business and assess the ML/TF risks of the respondent bank.

Information on a respondent bank's AML/CFT policies and procedures may be obtained from the respondent bank or from publicly available information (such as financial information, or any mandatory supervisory information relating to the respondent bank). The correspondent bank should verify the identity of the respondent bank using reliable, independent source documents, data or information and take measures to verify other CDD information on the respondent bank and identify any beneficial owners.

At account opening, correspondent banks may collect, and subsequently update, respondent banks' information by using third-party databases that contain relevant information on banks (often referred to as "KYC utilities")[3]. KYC utilities may provide efficiency gains for both correspondent and respondent banks to gather and provide information, especially with regard to standardisation and inter-operability (e.g. the ability of different systems to share data).

Correspondent banks should also consider gathering information from public sources. These may include the website of the supervisory authority of the respondent bank (e.g. public registers), for cross-checking identification data with the information obtained by the supervisor in the licensing process, or with regard to potential AML/CFT administrative sanctions that have been imposed on the respondent bank.

In assessing whether to enter into a correspondent banking relationship, the correspondent bank should also consider relevant information on the jurisdiction in which

[3] KYC Utilities are facilities managed by third-party platforms that aim to streamline the collection and exchange of data between banks and their customers, while maintaining appropriate privacy controls.

the respondent operates, for instance from international bodies or other sources. Where deficiencies are identified in certain jurisdictions, correspondent banks should also take into account the corrective measures under way to strengthen the jurisdiction's AML/CFT controls, as well as efforts by domestic authorities to instruct respondent banks on how to strengthen their controls and mitigate ML/TF risks. This would be relevant especially where a correspondent bank is considering whether an existing correspondent banking relationship could be subject to additional monitoring or restrictions, rather than termination.

Correspondents would also benefit from talking to potential respondent banks about how it is addressing these issues (i.e., implementing policies and procedures that go above and beyond the requirements of domestic laws and regulations to comply with international standards).

Where the correspondent institution has identified a correspondent banking relationship that poses a higher degree of risk, it should apply enhanced measures that are in line with the risks associated to that relationship. For example, in some circumstances, closer interaction (conference calls or face-to-face meetings) with the respondent institution's management and compliance officer(s) may be appropriate.

Although correspondent banks are not required to conduct KYCC, they should ensure that they are able to review and access a copy of the CDD information from their respondent bank upon request, and be satisfied their respondent bank has adequate ML/TF controls. In establishing a correspondent account, banks should always do their own CDD, and not rely on third parties. The ultimate responsibility for implementing AML/CFT measures remains with the correspondent institution.

Finally, the correspondent must obtain senior management or Board approval (as relevant) prior to the relationship being established.

5. MANAGING THE RISKS

ONGOING DUE DILIGENCE

Correspondent institutions should conduct ongoing due diligence of the correspondent banking relationship, including periodical reviews of the CDD information on the respondent institution. This ensures that that the information is kept up-to-date in line with the risk associated with the relationship. Where such reviews reveal changes in the risk profile of the respondent institution, the correspondent institution should consider whether it should adjust its risk assessment of the respondent institution and what further information may be needed to support this adjustment. The frequency with which periodic reviews are undertaken should depend on the level of risk associated with the respondent institution.

ONGOING TRANSACTION MONITORING

Transaction monitoring of respondent accounts can help mitigate the ML/TF risks arising from correspondent banking activities. Depending on the nature and scale of a bank's correspondent banking activity, automated AML transaction monitoring systems may be appropriate. Some of the activities to note include:

- Monitoring for sudden and/or significant changes in transaction activity by value or volume;

- Identifying hidden relationships – monitoring activity between accounts and customers (including respondents and their underlying customers), and identifying common beneficiaries and remitters amongst apparently unconnected accounts/respondents;
- Monitoring for significant increases of activity or consistently high levels of activity with (to or from) higher risk countries and/or entities; and
- Monitoring for activity that may indicate possible ML/TF, such as the structuring of transactions under reporting thresholds, or transactions in round amounts.

ONGOING MONITORING AND TRANSACTION INFORMATION REQUESTS

In situations where the correspondent bank's monitoring system flags a transaction, the correspondent institution should have internal process to further review the activity which could include requesting transaction information of the respondent institution to clarify the situation and possibly clear the alert.

The request for information could be targeted on the specific transaction that was flagged and could include, depending on the risk level of the transaction and associated parties, a request to access information about the customer of the respondent institution as a means to get a proper understanding of the reasonableness of the transaction. Some questions that could be asked, in this context, may include:

- Duration of customer's relationship with the respondent institution and whether the respondent institution classifies the customer as a high risk customer.
- Purpose of the account(s) maintained by the customer at the respondent, e.g. business, personal or other.
- Details of customer's parent company and the name(s) of the beneficial owner(s).
- Source of the funds of the customer.
- Consistency between the transactional history in the account profile of the customer, and his KYC data, or with any other information available to the respondent bank.
- Rationale of the transaction between the customer and a counterparty.
- Nature of the relationship between the customer and a counterparty.
- Possible affiliation of the customer with a third-party.
- Additional details regarding the goods/services being exchanged by the customer and third-parties that are not found directly in the payment details of the transaction that may explain it.
- Status of the bank account of the customer e.g. opened/closed.

Where the correspondent institution requests further information on a transaction from the respondent, the expectation is that the respondent will respond in a timely manner and provide documents/information to the level of detail requested. Non-compliance with such requests should trigger concerns for the correspondent that the respondent is unable to understand or manage its risks and may lead to the filing of a suspicious transaction report by the correspondent institution. A request for information could be followed by a reassessment of the respondent's business and risk profile where/when necessary. In cases in which the respondent bank is unable to provide a timely, suitably detailed response to assuage the correspondent's concerns, or if a pattern of non-responsiveness develops, the correspondent may opt to restrict or close the CBR with the respondent.

TERMS GOVERNING CORRESPONDENT BANKING RELATIONSHIPS

One way for correspondent institutions to manage their risks more effectively from the inception is to enter into a written agreement with the respondent institution before correspondent services are provided. The correspondent institution should at a minimum consider the following to be included in the terms:

- The method of monitoring the relationship to ascertain how effectively the respondent institution is applying CDD measures to its customers, and implementing AML/CFT controls;
- The products and services to be provided under the correspondent banking relationship;
- The respondent institution's responsibilities concerning compliance with AML/CFT requirements, permitted third-party usage of the correspondent account and applicable internal controls to these situations;
- In case of third party usage of correspondent accounts, any potential restrictions that the correspondent institution may want to place on the use of the correspondent account (e.g. limiting transaction types, volumes, etc.); and
- Conditions regarding the requests for information on particular transactions, especially in the case of "payable through accounts" relationships, and cases and procedures for terminating or limiting a business relationship.
- Establishing each institution's responsibilities for managing the risks associated with the relationship; and
- Ongoing substantive discussions about risk and risk management.

Written agreements have the advantage of documenting the intended purpose and use of correspondent banking relationships and allows the correspondent institution to demonstrate to its regulator some of the steps it has taken to understand the risks presented by its correspondent relationships.

The terms and conditions governing the correspondent banking relationship should include notice periods for terminating or limiting the business relationships. From the respondent bank's perspective, such notice periods should feed into the banks' business continuity plans. As part of contingency planning for critical functions, a respondent bank may consider having more than one correspondent banking account for its payment services, where necessary for its continued operation.

The decision to enter into a correspondent banking relationship with a respondent bank should be approved by the relevant senior management of the correspondent bank. When significant ML/TF risk factors emerge in an existing correspondent banking relationship, the correspondent should review the relationship. Following the review, the decision to continue the relationship with additional risk mitigation measures or to terminate it, should be escalated to the relevant senior management. Correspondent banks should consider filing an STR if they opt to restrict or terminate a correspondent relationship due to concerns at all related to AML/CFT compliance or sanctions evasion.

Correspondent banks should refuse to enter into or continue correspondent banking relationships with "shell" banks (i.e. banks incorporated in a jurisdiction in which they have no physical presence and which is unaffiliated with a regulated financial group). FATF has recommended that correspondent banks should enter into correspondent banking relationships only if they are satisfied that the respondent bank is not a shell bank.

Additionally, the correspondent bank should not enter into or continue correspondent banking relationship if the respondent bank is known to permit its accounts to be used by shell banks[4].

6. ONGOING COMMUNICATION

Correspondent banking relationships are, by their nature, based on mutual trust between the correspondent and the respondent institutions, particularly that AML/CFT controls are being effectively implemented by the respondent institution.

Consequently, it is important for correspondent institutions to maintain an ongoing and open dialogue with the respondent institutions, as well as help them understand the correspondent's AML/CFT policy and expectations, and when needed, engage with them to improve their AML/CFT controls and processes.

Such communication supports the monitoring requirement by helping to flag new and emerging risks and better understanding of the existing risks. This, in turn, would help to strengthen risk mitigation measures and any other incidental issues concerning exchange of information.

7. OTHER RISK MITIGATION MEASURES

THE INTERNAL AUDIT AND COMPLIANCE FUNCTIONS

A bank's Internal Audit and Compliance functions have important responsibilities in evaluating and ensuring compliance with procedures related to correspondent banking activities. Internal controls should cover identification measures of the respondent banks, the collection of information, the ML/TF risk assessment process, ongoing monitoring of correspondent banking relationships and compliance with the duties to detect and report suspicions (about respondents and/or possible underlying subjects involved in the transactions).

TRAINING

The bank must train staff on how correspondent banking transactions may be used for ML/TF, and include such information in its procedures for managing this risk. This training should be directed specifically at those staff directly involved in correspondent banking transactions and dealing with correspondent banking customers and should be risk focused.

SENIOR MANAGEMENT

Senior management should also be aware of the roles and responsibilities of the different functions within the bank (e.g. the business divisions, Compliance Officers including the Group AML/CFT Officer, Audit) pertaining to correspondent banking activities.

[4] Please see Section 312 of the USA PATRIOT Act (enhanced due diligence for correspondent accounts maintained for certain foreign banks)

GROUP POLICIES

If a respondent bank has correspondent banking relationships with several entities belonging to the same group, the Head Office of the group should ensure that the assessments of the risks by the different entities of the group are consistent with the group-wide risk assessment policy. The group's head office should coordinate the monitoring of the relationship with the respondent bank, particularly in the case of a high-risk relationship, and make sure that adequate information-sharing mechanisms are in place.

If a correspondent bank has business relationships with several entities belonging to the same group but established in different host countries, the correspondent bank should take into account the fact that these entities belong to the same group. However, the correspondent bank should also independently assess the ML/TF risks presented by each business relationship.

8. RESOURCES

The hyperlinks below are provided for convenience, and were current at the time of publication of this guidance. Readers are cautioned that these may be subject to change without notice by the relevant site owners.

BCBS
Sound management of risks related to money laundering and financing of terrorism, June 2017
http://www.bis.org/bcbs/publ/d405.pdf

Financial Action Task Force
Correspondent Banking Services
October 2016
http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Correspondent-Banking-Services.pdf

Financial Action Task Force
The 40 Recommendations
June 2017
http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

The Wolfsberg Group
Anti-Money Laundering Principles for Correspondent Banking
2014
http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg-Correspondent-Banking-Principles-2014.pdf

Financial Conduct Authority
Banks' management of high money-laundering risk situations
June 2011
http://www.fsa.gov.uk/pubs/other/aml_final_report.pdf

Joint Money Laundering Steering Group
Guidance on correspondent banking
http://www.jmlsg.org.uk/industry-guidance/article/jmlsg-guidance-current

International Monetary Fund
Recent trends in correspondent banking relationships – Further considerations, March 2017
https://www.imf.org/~/media/Files/Publications/PP/031617.ashx

Financial Services Authority, UK
Banks' management of high money-laundering risk situations
https://www.fca.org.uk/publication/corporate/fsa-aml-final-report.pdf

9. ANNEXURE 1: CONSOLIDATED EXAMPLES OF GOOD AND POOR PRACTICE – CORRESPONDENT BANKING RELATIONSHIPS

Examples of good practice	*Examples of bad practice*
Risk assessment of respondent banks	
▪ Regularly assessments of correspondent banking risks taking into account various money laundering risk factors such as the country (and its AML regime); ownership/management structure (including the possible impact/influence that ultimate beneficial owners with political connections may have); products/operations; transaction volumes; market segments; the quality of the respondent's AML systems and controls and any adverse information known about the respondent. ▪ More robust monitoring respondents identified as presenting a higher risk. ▪ Risk scores that drive the frequency of relationship reviews. ▪ Taking into consideration publicly available information from national government bodies and non-governmental organisations and other credible sources.	▪ Failing to consider the money-laundering risks of correspondent relationships. ▪ Inadequate or no documented policies and procedures setting out how to deal with respondents. ▪ Applying a 'one size fits all' approach to due diligence with no assessment of the risks of doing business with respondents located in higher risk countries. ▪ Failing to prioritise higher risk customers and transactions for review. ▪ Failing to take into account high-risk business types such as money service businesses and offshore banks
Customer onboarding	
▪ Assigning clear responsibility for the CDD process and the gathering of relevant documentation. ▪ EDD for respondents that present greater risks or where there is less publicly available information about the respondent. ▪ Gathering enough information to understand customer details; ownership and management; products and offerings; transaction volumes and values; customer market segments; customer reputation; as well as the AML control environment.	▪ Inadequate CDD on parent banks and/or group affiliates, particularly if the respondent is based in a high-risk jurisdiction. ▪ Collecting CDD information but failing to assess the risks. ▪ Over-relying on the Wolfsberg Group AML questionnaire. ▪ Failing to follow up on outstanding information that has been requested during the CDD process. ▪ Fail to follow up on issues identified during the CDD process ▪ Relying on parent banks to conduct CDD for a correspondent account and taking no steps to ensure this has been done.

▪ Screening the names of senior managers, owners and controllers of respondent banks to identify PEPs and assessing the risk that identified PEPs pose. ▪ Independent quality assurance work to ensure that CDD standards are up to required standards consistently across the bank. ▪ Discussing with overseas regulators and other relevant bodies about the AML regime in a respondent's home country. ▪ Identifying risk in particular business areas (e.g. informal value transfer such as 'hawala', tax evasion, corruption) through discussions with overseas regulators. ▪ Visiting, or discuss with, respondent banks to discuss AML issues and gather CDD information. ▪ Gathering information about procedures at respondent firms for sanctions screening and identifying/managing PEPs. ▪ Understanding respondents' processes for monitoring account activity and reporting suspicious activity. ▪ Requesting details of how respondents manage their own correspondent banking relationships. ▪ Senior management/senior committee sign-off for new correspondent banking relationships and reviews of existing ones.	▪ Collecting AML policies etc. but making no effort to assess them. ▪ Having no information on file for expected activity volumes and values. ▪ Failing to consider adverse information about the respondent or individuals connected with it. ▪ No senior management involvement in the approval process for new correspondent bank relationships or existing relationships being reviewed.
Ongoing monitoring of respondent accounts	
▪ Review periods driven by the risk rating of a particular relationship; with high risk relationships reviewed more frequently. Obtaining an updated picture for the purpose of the account and expected activity. ▪ Updating screening of respondents and connected individuals to identify individuals/entities with PEP connections or on relevant sanctions lists.	▪ Copying periodic review forms year after year without challenge from senior management. ▪ Failing to take account of any changes to key staff at respondent banks. ▪ Carrying out annual reviews of respondent relationships but fail to consider money-laundering risk adequately. ▪ Failing to assess new information gathered during ongoing monitoring of a relationship.

▪ Involving senior management and AML staff in reviews of respondent relationships and consideration of whether to maintain or exit high risk relationships. ▪ Where appropriate, using intelligence reports to help decide whether to maintain or exit a relationship. ▪ Carrying out ad-hoc reviews in light of material changes to the risk profile of a customer.	▪ Failing to consider money laundering alerts generated since the last review. ▪ Relying on parent banks to carry out monitoring of respondents without understanding what monitoring has been done or what the monitoring found. ▪ Failing to take action when respondents do not provide satisfactory answers to reasonable questions regarding activity on their account. ▪ Focusing too much on reputational or business issues when deciding whether to exit relationships with respondents which give rise to high money-laundering risk.

SOURCE: FSA, UK

ANNEX 2 - CHANNELING PAYMENTS THROUGH THE SWIFT NETWORK

CBR arrangements involve the exchange of message between banks, including through the SWIFT network. These messages could be associated with payments, trade finance, foreign exchange, or securities transactions. The most commonly used standard for cross-border payments is SWIFT.

Box 1: SWIFT: What's in a Message?

Standards Message Types (MT) have been developed to support the business transactions of SWIFT users. To ensure that the multitude of practices and conventions of users are in harmony, financial messages transmitted via the SWIFT network must adhere to the message text standards. Standards enable financial institutions to move from manual to automated initiation and processing of financial transactions.

SWIFT messages are grouped into ten major categories. This includes the following: (i) customer payments and checks; (ii) financial institution transfers; (iii) treasury markets, covering foreign exchange, money markets, and derivatives; (iv) collections and cash letters; (v) securities markets; (vi) commodities and syndications; (vii) documentary credits and guarantees; (viii) travelers checks; (ix) cash management and customer status; and (x) common group messages. An MT is composed of three digits, which generally define its category, group, and type. Group describes the function of the message. Type describes the specific function. Examples of common message types are as follows:

- ✓ MT 103—Single customer transfer, which instructs a funds transfer;
- ✓ MT 202—General financial institution transfer, which request the movement of funds between financial institutions except if the transfer is related to an underlying customer credit transfer that was sent with the cover method, in which case the MT 202 COV must be used;
- ✓ MT 202 COV—General financial institution transfer, which requests the movement of funds between financial institutions, related to an underlying customer credit transfer that was sent with the cover method;
- ✓ MT 300—Foreign exchange confirmation on agreement to buy and sell two currencies; and
- ✓ MT 700—Issuance of a documentary credit, indicating the terms and conditions.

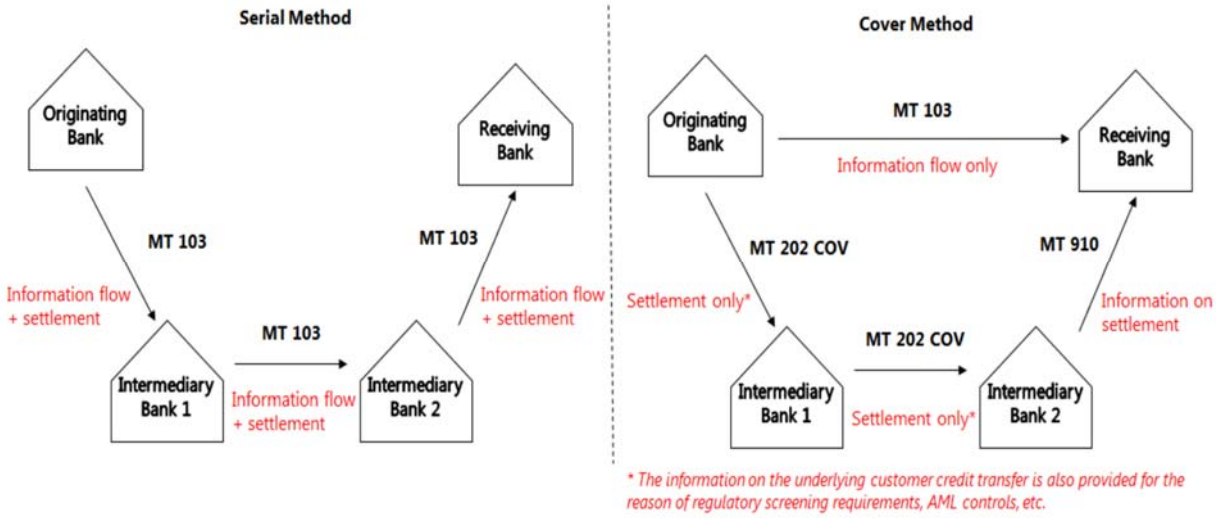
Source: SWIFT.

3. There are two methods in channelling payments through the SWIFT network. This includes the serial and cover methods.
   1) The serial method involves sending an MT 103 (or equivalent) from the originating bank to the receiving bank through one or more intermediaries.

Each pair along the payment chain has a direct account relationship. The payment information and the settlement instruction travel together in the MT 103 message.

2) 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 CBRs.
3) The transparency of ordering customers and final beneficiaries underlying payment instructions was further enhanced with new message standards, called MT 202 COV, which helps improve the screening of transactions by intermediary banks against AML/CFT and sanctions requirements.

Both methods are used in practice when an originating bank has no bilateral account relationship with the receiving bank, and can help fulfil compliance with AML/CFT and other relevant regulatory requirements provided that all relevant payment fields of the respective payment message are accurately completed.



Source: IMF –recent trends in correspondent banking activities.