16: Correspondent banking

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

This sectoral guidance considers specific issues over and above the more general guidance set out in Part I, Chapters 4, 5, and 7, which firms engaged in correspondent banking should take into account when considering applying a risk-based approach.

Overview of the sector

16.1 For the purposes of this guidance, correspondent banking is defined as the provision of banking-related services by one bank (Correspondent) to an overseas bank (Respondent) to enable the Respondent to provide its own customers with cross-border products and services that it cannot provide them with itself, typically due to a lack of an international network.

16.2 Correspondent banking activity can include establishing accounts, exchanging methods of authentication of instructions (e.g. by exchanging SWIFT or telex test keys and/or authorised signatures) and providing payment or other clearing-related services. A correspondent relationship can be based solely on the exchange of test keys, with cover for direct payment instructions being arranged through a third bank for credit to the Correspondent's/Respondent's own account in another jurisdiction. Activity can also encompass trade-related business and treasury/money market activities, for which the transactions can be settled through the correspondent relationship. The scope of a relationship and extent of products and services supplied will vary according to the needs of the Respondent, and the Correspondent's ability and willingness to supply them. Credit, operational and reputational risks also need to be considered.

16.3 A Correspondent is effectively an agent (intermediary) for the Respondent and executes/processes payments or other transactions for customers of the Respondent. The underlying customers may be individuals, corporates or even other financial services firms. Beneficiaries of transactions can be customers of the Correspondent, the Respondent itself or, in many cases, customers of other banks.

What are the money laundering risks in correspondent banking?

16.4 The Correspondent often has no direct relationship with the underlying parties to a transaction and is therefore not in a position to verify their identities. Correspondents often have limited information regarding the nature or purpose of the underlying transactions, particularly when processing electronic payments (wire transfers – see Part 1, paragraph 5.2.10 - 5.2.13) or clearing cheques. For these reasons, correspondent banking is in the main non face-to-face business and must be regarded as high risk from a money laundering and/or terrorist financing perspective. Firms undertaking such business are required by the ML Regulations (Regulation 10) "to apply on a risk-sensitive basis enhanced customer due diligence measures". These requirements are addressed in this guidance.

16.5 Correspondent banking relationships, if poorly controlled, can allow other financial services firms with inadequate AML/CTF systems and controls, and customers of those firms, direct access to international banking systems.

16.6 A Correspondent handling transactions which represent the proceeds of criminal activity or terrorist financing risks regulatory fines and/or damage to its reputation.

How to assess the elements of risk in correspondent banking

16.7 For any Correspondent, the highest risk Respondents are those that:

- are offshore banks that are limited to conducting business with non residents or in non local currency, and are not subject to robust supervision of their AML/CTF controls; or
- are domiciled in jurisdictions with weak regulatory/AML/CTF controls or other significant reputational risk factors e.g., corruption.

16.8 Correspondents must not maintain relationships with Respondents that are shell banks (see Part I, paragraphs 5.3.65 – 5.3.67) nor any Respondent which provides banking services to shell banks.

16.9 Enhanced customer due diligence (see Part I, section 5.5) must be undertaken on Respondents (and/or third parties authorised exceptionally to provide instructions to the Correspondent e.g., other entities within a Respondent group) using a risk-based approach. The following risk indicators should be considered both when initiating a relationship, and on a continuing basis thereafter, to determine the levels of risk-based due diligence that should be undertaken:

- **The Respondent's domicile.** The jurisdiction where the Respondent is based and/or where its ultimate parent is headquartered may present greater risk (or may mitigate the risk, depending on the circumstances). Certain jurisdictions are recognised internationally as having inadequate anti-money laundering standards, insufficient regulatory supervision, or presenting greater risk for crime, corruption or terrorist financing. Other jurisdictions, however, such as many members of the Financial Action Task Force (FATF), have more robust regulatory environments, representing lower risks. Correspondents should review pronouncements from regulatory agencies and international bodies such as the FATF, to evaluate the degree of risk presented by the jurisdiction in which the Respondent and/or its parent are based.

- **The Respondent's ownership and management structures.** The location of owners, their corporate legal form and/or a lack of transparency of the ultimate beneficial ownership are indicative of the risk the Respondent presents. Account should be taken of whether the Respondent is publicly or privately owned; if publicly held, whether its shares are traded on a recognised market or exchange in a jurisdiction with a satisfactory regulatory regime, or, if privately owned, the identity of any beneficial owners and controllers. Similarly, the location and experience of management may indicate additional concerns, as would unduly frequent management turnover. The involvement of PEPs in the management or ownership of certain Respondents may also increase the risk.

- **The Respondent's business and customer base**. The type of business the Respondent engages in, as well as the type of markets it serves, is indicative of the risk the Respondent presents. Involvement in certain business segments that are recognised internationally as particularly vulnerable to money laundering, corruption or terrorist financing, may present additional concern. Consequently, a Respondent that derives a substantial part of its business income from higher risk customers may present greater risk. Higher risk customers are those customers that may be involved in activities, or are connected to jurisdictions, that are identified by credible sources as

activities or countries being especially susceptible of money laundering/terrorist financing or corruption.

- **Downstream Correspondent Clearing**. A Downstream Correspondent Clearer is a Respondent that receives correspondent banking services from a Correspondent and itself provides correspondent banking services to other financial institutions in the same currency as the account it maintains with its Correspondent. When these services are offered to a Respondent that is itself a Downstream Correspondent Clearer, a Correspondent should, on a risk-based approach, take reasonable steps to understand the types and risks of financial institutions to whom the Respondent offers such services, especial care being taken to ensure there are no shell bank customers, and consider the degree to which the Respondent examines the anti-money laundering/terrorist financing controls of those financial institutions.

Customer due diligence

16.10 All correspondent banking relationships with Respondents from non-EEA states must be subject to an appropriate level of due diligence which as a minimum meets the requirements laid down in Regulation 14 (3) of the ML Regulations and additionally will ensure that a Correspondent is comfortable conducting business with/for a particular Respondent (and hence its underlying customers) given the Respondent's risk profile. It may be appropriate for a Correspondent to take some comfort from the fact that a Respondent domiciled in or operating in a regulatory environment that is recognised internationally as adequate in the fight against money laundering/terrorist financing and corruption. In these instances, a Correspondent may choose to rely on publicly available information obtained either from the Respondent itself, another reputable existing Respondent, from other credible sources (e.g., regulators, exchanges), or from reputable information sources, to satisfy its due diligence requirements.

16.11 The extent of the correspondent relationship should be factored into the level of due diligence undertaken. A Correspondent, subject to its risk-based approach, may decide not to undertake more than the minimum level of due diligence set out in Regulation 14 (3) for limited correspondent relationships, such as the exchange of test keys.

16.12 The verification of identity of Respondents should be undertaken in accordance with Part I, Chapter 5. Their ownership structures should be ascertained and understood and, for those privately-owned Respondents where it is appropriate to identify significant owners and/or controllers (beneficial owners), the form of evidence and information gathered on such owners and controllers must be sufficient, on a cumulative basis, to confirm identity with reasonable certainty.

16.13 A Correspondent's policies and procedures should require that the information, including due diligence, held relating to a Respondent is periodically reviewed and updated. The frequency of review should be tailored to the perceived risks, and updating should be undertaken as a result of trigger events e.g. an extension to the service/product range provided; a material change to the nature/scope of business undertaken by the Respondent; or as a result of significant changes to its legal constitution, or its owners or controllers or negative regulatory pronouncements and/or press coverage.

16.14 The level and scope of due diligence undertaken should take account of the relationship between the Respondent and its ultimate parent (if any). In general, for relationships maintained with branches, subsidiaries or affiliates, the status, reputation and controls of the parent entity should be considered in determining the extent of due diligence required on the Respondent. Where the Respondent is located in a high-risk jurisdiction, Correspondents may consider it appropriate to conduct additional due diligence on the Respondent as well

as the parent. In instances when the Respondent is an affiliate that is not substantively and effectively controlled by the parent, then the quality of the affiliate's AML/CTF controls should always be established.

16.15 The Correspondent in assessing the level of due diligence to be carried out in respect of a particular Respondent, (in addition to the issues raised in paragraph 16.9) must consider:

- **Regulatory status and history.** The primary regulatory body responsible for overseeing or supervising the Respondent and the quality of that supervision. If circumstances warrant, a Correspondent should also consider publicly available materials to ascertain whether the Respondent has been the subject of any criminal case or adverse regulatory action in the recent past.

- **AML/CTF controls.** A Correspondent should establish whether the Respondent is itself regulated for money laundering/terrorist financing prevention and, if so, whether the Respondent is required to verify the identity of its customers and apply other AML/CTF controls to FATF standards/equivalent to those laid down in the money laundering directive. Where this is not the case, additional due diligence should be undertaken to ascertain and assess the effectiveness of the Respondent's internal policy on money laundering/terrorist financing prevention and its know your customer and activity monitoring controls and procedures. Where undertaking due diligence on a branch, subsidiary or affiliate, consideration may be given to the parent having robust group-wide controls, and whether the parent is regulated for money laundering/terrorist financing to FATF standards/equivalent to those laid down in the money laundering directive. If not, the extent to which the parent's controls meet FATF standards/equivalent to those laid down in the money laundering directive and whether these are communicated and enforced 'effectively' throughout its network of international offices, should be ascertained.

- **Shell banks.** Whether the Respondent has confirmed that it will not provide banking services to or engage in business with, shell banks.

16.16 Prior to establishing a new correspondent relationship a person from senior management and independent from, the officer sponsoring the relationship must approve the setting up of the Respondent's account. For higher risk relationships, the Correspondent's compliance (or MLRO) function should also satisfy itself that the risks are acceptable.

Enhanced due diligence

16.17 Correspondents are required by Regulation 14(3) of the ML Regulations to subject Respondents from non-EEA States to enhanced customer due diligence, but should consider doing so whenever the Respondent has been considered to present a greater money laundering/terrorist financing risk. The enhanced due diligence process should involve further consideration of the following elements designed to ensure that the Correspondent has secured a greater level of understanding:

- **Respondent's ownership and management.** For all beneficial owners and controllers, the sources of wealth and background, including their reputation in the market place, as well as recent material ownership changes (e.g. in the last three years). Similarly, a more detailed understanding of the experience of each member of executive management as well as recent material changes in the executive management structure (e.g., within the last three years).

- **Respondent's business.** Gather sufficient information about the Respondent to understand fully the nature of its business. In addition, determine from publicly-available information the reputation of the Respondent and the quality of its supervision.

- **PEP involvement.** If a PEP (see Part I, paragraphs 5.5.18-5.5.30) appears to have a material interest or management role in a Respondent then the Correspondent should ensure it has an understanding of that person's role in the Respondent.

- **Respondent's anti-money laundering/terrorist financing controls.** An assessment of the quality of the Respondent's AML/CTF and customer identification controls, including whether these controls meet internationally recognised standards. The extent to which a Correspondent should enquire will depend upon the perceived risks. Additionally, the Correspondent may wish to speak with representatives of the Respondent to obtain comfort that the Respondent's senior management recognise the importance of anti-money laundering/terrorist financing controls.

- **Document the relationship.** Document the respective responsibilities of the Respondent and Correspondent.

- **Customers with direct access to accounts of the Correspondent.** Be satisfied that, in respect of these customers, the Respondent:
  - (i) has verified the identity of, and performs ongoing due diligence on, such customers; and
  - (ii) is able upon request to provide relevant customer due diligence data to the Correspondent.

Monitoring

16.18 Implementing appropriate documented monitoring procedures can help mitigate the money laundering risks for firms undertaking correspondent banking activities. General guidance on monitoring is set out in Part 1, section 5.7.

16.19 The level of monitoring activity undertaken by a Correspondent on its Respondent's activity through it should be commensurate with the risks posed by the Respondent. Due to the significant volumes that correspondent banking activity can entail, together with the need to work within prescribed scheme settlement deadlines, electronic and/or post-execution monitoring processes are often the norm.

16.20 The following possible techniques of monitoring activity combine to represent electronic monitoring good practice in the area of correspondent banking relationships:

- <u>Anomalies in behaviour</u>
  - Monitoring for sudden and/or significant changes in transaction activity by value or volume.

- <u>Hidden relationships</u>
  - Monitor for activity between accounts, customers (including Respondents and their underlying customers). Identify common beneficiaries and remitters or both amongst apparently unconnected accounts/Respondents. This is commonly known as link analysis.

- High risk geographies and entities
  - Monitoring for significant increases of activity or consistently high levels of activity with (to or from) higher risk geographies and/or entities.

- Other money laundering behaviours
  - Monitoring for activity that may, in the absence of other explanation, indicate possible money laundering, such as the structuring of transactions under reporting thresholds, or transactions in round amounts

- Other considerations
  - In addition to the monitoring techniques above, the monitoring system employed to monitor correspondent banking for AML/CTF purposes should facilitate the ability to apply different thresholds against customers that are appropriate to their particular risk category.

Other monitoring activity

16.21 In addition to monitoring account/transaction activity, a Correspondent should monitor a Respondent for changes in its nature and status. As such, information about the Respondent collected during the customer acceptance and due diligence processes must be:

- Reviewed and updated on a periodic basis. (Periodic review of customers will occur on a risk-assessed basis), or
- Reviewed on an ad hoc basis as a result of changes to the customers information identified during normal business practices, or
- Reviewed when external factors result in a material change in the risk profile of the customer.

16.22 Where such changes are identified, the Respondent should be subject to a revised risk assessment, and a revision of their risk categorisation, as appropriate. Where, as a result of the review, the risk categorisation is altered (either up or down) a firm should ensure that the due diligence standards for the Respondent's new risk categorisation are complied with, by updating the due diligence already held. In addition, the level of monitoring undertaken should be adjusted to that appropriate for the new risk category.

16.23 Firms should consider terminating the accounts of Respondents, and consider their obligation to report suspicious activity, for Respondents who fail to provide satisfactory answers to reasonable questions regarding transactions/activity passing through the correspondent relationship, including, where appropriate, the identity of their customers featuring in unusual or suspicious transactions or activities.

16.24 The firm will need to have a means of assessing that its risk mitigation procedures and controls are working effectively. In particular the firm will need to consider:

- Reviewing ways in which different services may be used for ML/TF purposes, and how these ways may change, supported by typologies/law enforcement feedback, etc;
- Adequacy of staff training and awareness;
- Capturing appropriate management information;
- Upward reporting and accountability; and
- Effectiveness of liaison with regulatory and law enforcement agencies.

Staff awareness, training and alertness

16.25 The firm must train staff on how correspondent banking transactions may be used for ML/TF and in the firm's 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 clients and should be tailored around the greater risks that this type of business represents. Whilst there is no single solution when determining how to deliver training, training of relationship management staff via workshops may well prove to be more successful than on-line learning or videos/CDs.