

P O Box 427 Pretoria 0001 South Africa

370 Helen Joseph Street Pretoria 0002

+27 12 313 3911 / 0861 12 7272

www.resbank.co.za



SOUTH AFRICAN RESERVE BANK
Prudential Authority

Ref.: 15/8/2

G7/2022

To: All banks, branches of foreign institutions, controlling companies, eligible institutions and auditors of banks or controlling companies

Guidance Note issued in terms of section 6(5) of the Banks Act 94 of 1990

Guidelines for matters related to the prevention of banks or controlling companies being used for any money laundering or other unlawful activity in respect of correspondent banking relationships.

Executive summary

The purpose of this Guidance Note is to provide guidance to banks, branches of foreign institutions, controlling companies, eligible institutions, and auditors of banks or controlling companies on anti-money laundering and counter terrorist financing risk management practices related to correspondent banking relationships.

Section 64A of the Banks Act 94 of 1990 (Banks Act) read with regulations 39, 50 and 36(17)(b) of the Regulations relating to Banks (Regulations) requires that in relation to any cross-border correspondent banking or other similar relationship, the bank or controlling company should have in place robust due diligence procedures and measures.

This Guidance Note also sets out practices and guidelines to assist banks and controlling companies (hereinafter collectively referred to as banks) with anti-money laundering and counter terrorist financing risk management and compliance programme (RMCP) requirements in terms of the Financial Intelligence Centre Act 38 of 2001 (FIC Act).

1 Introduction

1.1 Correspondent banking is the provision of banking-related services by one bank (the correspondent bank) to another bank (the respondent bank).¹ The respondent bank (RB) is typically based in another country in relation to the correspondent bank (CB). The CB has the ability to enable a RB to provide clients of the RB with access to cross-border products and services that it cannot provide to its own clients and enables its clients to make payments in foreign currencies. Often these products and services include the establishment of foreign currency accounts and the exchange of authentication of instructions, for example via Society for

¹ <https://www.fatf-gafi.org/glossary/>

Worldwide Interbank Financial Telecommunication (SWIFT), as well as payment-and/or clearing-related services. Trade-related transactions typically allow for the settlement of transactions through correspondent banking relationships (CBRs).

- 1.2 Financial Action Task Force (FATF) Recommendation 10 states that financial institutions (FIs) should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names. It further states that FIs should be required to undertake customer due diligence (CDD) measures in certain circumstances.
- 1.3 FATF Recommendation 13 states that FIs should be required, in relation to cross-border correspondent banking and other similar relationships, in addition to performing CDD or enhanced due diligence (EDD) measures, take further steps to understand the respondent institution's activities and implemented anti-money laundering and counter financing of terrorism (AML/CFT) controls. It further prohibits FIs from entering into, or continuing, a CBR with shell banks².
- 1.4 FATF Recommendation 16 states that countries should ensure that FIs 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.
- 1.5 The legislative framework in South Africa supports international AML/CFT principles for CBRs and includes the FATF's Recommendations, Wolfsberg principles and other best practices.
- 1.6 Regulation 36(17)(b)(ii) of the Regulations provides that every relevant foreign branch, subsidiary or operation of the bank or controlling company implements and applies AML/CFT measures consistent with the relevant FATF Recommendations. Furthermore, the higher of the AML/CFT standards applied in South Africa or the relevant host country must be followed.
- 1.7 Regulation 36(17)(b)(iii) of the Regulations further states that in relation to any cross-border CB or other similar relationship, the bank or controlling company must have in place robust due diligence procedures and measures. In addition, the bank or controlling company must gather sufficient information about a respondent institution, inter alia, to fully understand the nature of the respondent's business, to determine the reputation of the relevant institution, to determine the quality of supervision, including whether it has been subject to any money laundering (ML) or terrorist financing (TF) investigation or regulatory action, to ensure that the respondent institution does not permit its accounts to be used by a shell bank, assesses the respondent institution's AML/CFT controls, obtains the required approval from its senior management before it establishes any new CBR, duly documents the respective responsibilities of each relevant institution, with respect to payable through accounts (PTAs), be satisfied that the RB has duly verified the identity of and performed ongoing due diligence on any customer that has direct access to accounts of the correspondent bank, and that it is able to provide relevant customer identification data upon request to the CB.

² FATF Recommendations (Glossary): a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.

- 1.8 Regulation 47(2) of the Regulations states that a bank shall report an offence, which includes AML/CFT activity in which the bank was involved, and which was not identified in a timely manner and reported as required by law, including in terms of the requirements contained in the FIC Act.
- 1.9 Regulation 50 of the Regulations requires that a bank shall implement and maintain robust structures, policies, processes, and procedures to prevent it from being used for purposes of market abuse such as insider trading and market manipulation, and/or financial crimes such as financing of terrorist activities and ML.
- 1.10 The Prudential Authority (PA) assesses the adequacy of a bank or controlling company's policies, processes, systems, and procedures related to AML/CFT, and the bank or controlling company's compliance with relevant legislation, as an integral part of the PA's supervisory processes.
- 1.11 In this regard, regulation 38(4) of the Regulations states, among others, when the PA is of the opinion that a bank's policies, processes, and procedures relating to its risk assessment or internal control systems are inadequate, the PA may require the bank, among others-
- 1.11.1 to strengthen the bank's risk management policies, processes, or procedures; or
- 1.11.2 to strengthen the bank's internal control systems.
- 1.12 Section 21 of the FIC Act requires that an accountable institution (AI) must establish and verify the identity of its client prior to establishing a business relationship or concluding a single transaction with the client or the representatives of the client.
- 1.13 Section 42 of the FIC Act provides that an AI, which includes financial institutions- must develop, document, maintain and implement a programme for AML/CFT risk management and compliance. It further states that a RMCP must enable the AI to identify, assess, monitor, mitigate and manage the risk provision of products or services which may involve or facilitate ML/TF and related activities. Most importantly, the AI must indicate in its RMCP if any paragraphs of section 42(2) of the FIC Act are not applicable to it and the reason why such is not applicable.³
- 1.14 The Wolfsberg Group is a body that seeks to develop financial industry standards for AML/CFT policies. One such consideration being CBs as they play an integral part in the facilitation of cross-border payments. Given that the cross-border correspondent banking services are deemed to expose banks to higher AML/CFT risks, the Wolfsberg Correspondent Banking Due Diligence Questionnaire⁴ has been developed to address CB relationships that impact banks. CDD measures set out in the questionnaire provide some insight in terms of types of minimum requirements for achieving adherence to compliance and risk management obligations. Such guidelines if followed appropriately may contribute towards the reduction of de-risking of CBRs and greater inclusion of banks that would have otherwise generally been deemed undesirable.

³ Section 42(2A) of the FIC Act

⁴ <https://www.wolfsberg-principles.com/wolfsbergcb>

- 1.15 The Basel Committee on Banking Supervision (BCBS) has issued guidelines regarding sound management of risks related to ML and financing of terrorism⁵ which provide guidance on expectations concerning CBRs and the treatment thereof.

2 Risk Indicators

- 2.1 Correspondent banking risk factors that may guide the CB to identify, assess and monitor ML/TF/proliferation financing (PF) risks, inter alia, include the following:
- 2.1.1 ML/TF/PF risk(s) associated with a particular RB and/or the head office of the RB, which are regarded as unacceptable by the CB in accordance with its risk appetite;
 - 2.1.2 a weak AML/CFT or counter proliferation financing (CPF) regime associated with the country or region in which the RB is located;
 - 2.1.3 a lack of resources and/or effective controls dedicated to countering ML/TF/PF within the RB;
 - 2.1.4 poor understanding and a lack of adequate transaction monitoring controls in respect of inflows and outflows stemming from correspondent banking related transactions; and
 - 2.1.5 concerns of possible penalties by regulators for parties involved in the CBR in instances where one of the parties has insufficient or weak financial crime controls.

3 Obligations of parties to a CBR

- 3.1 Onboarding: The establishment of CBRs
- 3.1.1 CBs cannot establish or maintain CBRs with shell banks.
 - 3.1.2 CBs should not enter into CBRs if they are not satisfied, based on the information gathered or received, that the RB is not a shell bank.
 - 3.1.3 It is important that a CB has in place appropriate policies, procedures and systems which outline the business relationship agreements which define the roles and responsibilities of both the CB and the RB.
 - 3.1.4 The decision to enter into a CBR with a RB should be approved by the relevant senior management of the CB. There should be formal contractual relationships governing the CBR. Banks may elect to have contingency arrangements in the form of other CBRs in the event that a particular party to the contract wishes to terminate the CBR.
 - 3.1.5 A bank that wishes to enter into a vostro⁶ CBR must clearly understand, consider and assess the ML/TF/PF risks presented via such relationships and that ascertain that there are adequate due diligence procedures followed prior to the establishment of and during the CBR.
 - 3.1.6 A CB must be in a position to evidence sufficient understanding of the RB with whom it seeks to establish a relationship. This requires an understanding of various aspects linked to the RB to inform the inherent ML/TF/PF risks of such a relationship by giving consideration to, for example:
 - 3.1.6.1 The inherent ML/TF/PF risk resulting from the nature of the services provided (e.g., purpose of the services to be rendered such as trade finance/forex services/nesting or downstream payments/PTAs etc.);

⁵ Guidelines on the Sound management of risks related to money laundering and financing of terrorism <https://www.bis.org/bcbs/publ/d505.pdf> (Annexure 2)

⁶ A nostro account is one whereby a bank holds an account in a foreign currency at another bank. A vostro account is one whereby a bank holds an account for a foreign bank to enable the processing of payments of clients of the foreign bank in a differing currency.

- 3.1.6.2 The characteristics of the RB (e.g., the RB's major business activities including target markets and overall types of clients served in key business lines, the management, and beneficial owners of the RB and/or the regulatory status of the RB to be engaged);
- 3.1.6.3 The environment within which the RB operates (e.g. the jurisdiction in which the RB operates, including the jurisdiction where its parent company is located; the jurisdictions in which subsidiaries and branches of the group may be located (i.e., possibly using the group structure available in the Legal Entity Identifier (LEI) system), the jurisdictions in which third parties using the CBR may be located, the quality and/or effectiveness of banking regulation and supervision in the respondent's country (especially AML/CFT laws and regulations);
- 3.1.6.4 Whether the RB is situated in a high-risk jurisdiction or in jurisdictions with known strategic ML/TF deficiencies;
- 3.1.6.5 The type of clients and transactions the CB is expected to process in respect of the RB;
- 3.1.6.6 The evidence of the deliberation of the beneficial ownership (BO) structure of the RB and any specific concerns regarding the BO of the RB;
- 3.1.6.7 If the RB is a subsidiary that forms part of a group, how well does the subsidiary bank align to group standards and apply the higher of host or home principles?
- 3.1.6.8 Whether the RMCP (e.g., payment screening, client screening and transaction monitoring systems as well as other related policies and procedures) employed by the RB is adequate and in line with the risk appetite of the CB;
- 3.1.6.9 Whether transactions for high-risk client types will be processed (e.g., politically exposed persons, state owned entities, intermediaries, virtual-asset traders etc.);
- 3.1.6.10 Whether transactions for clients in high-risk industries will be processed (e.g., arms, weapons manufacturing, non-profit organisations etc.);
- 3.1.6.11 Whether the transactions are facilitating import or export trade in high-risk products or goods and if the ultimate destinations are understood; and/or
- 3.1.6.12 Consideration of the secrecy policies, if any, in the country of the RB.

4 Ongoing due diligence and monitoring

- 4.1 Through the application of a risk-based approach (RBA), in line with the risk profile of the CBR and as part of the RMCP adopted by a bank, all CBRs should be subjected to regular reviews to ensure that the information held in respect of the RB is up to date and valid. This is critical for CBs given that a CB will process payments on behalf of clients that are not of its own. Conversely, a RB often relies on a foreign bank to process payments on its behalf and should also be assured of the bank on which it relies to effect payments.
- 4.2 It is important to bear in mind that due diligence is more than identification and verification; there are various elements and bringing the different elements of CDD together will better enable a bank to know its client, who benefits from the transactions, the nature of the business in respect of which transactions are processed and to be able to determine suspicious or unusual activity and/or transactions by having adequate information to be in a position to make such determination. CDD should be sufficient to enable a bank to understand its customer and its activities.

- 4.3 A CB must assess the RB's AML/CFT controls on a risk-sensitive basis and understand the RB's AML/CFT policies, procedures and systems, including sanctions screening measures, payment screening measures, and ascertain if there are sufficient oversight functions testing the efficacy of AML/CFT controls linked to these areas e.g., compliance or audit reviews undertaken.
- 4.4 RBs and CBs should have adequate transaction monitoring measures in place to detect financial activity that is inconsistent with the purpose of the services provided to the RB or any financial activity that is contrary to commitments that may have been concluded between the CB and the RB.
- 4.5 The CB must consider liaising directly (e.g., by phone or videoconference) with the RB's local management and compliance officer, or potentially by an on-site visit to gain the assurance required. The frequency of this will depend on the risk rating assigned to the specific CBR with the RB (e.g., banks with nested relationships based in high-risk jurisdictions or with PTA⁷ may be factors that contribute to a higher risk rating and thus more frequent monitoring and due diligence is required). EDD must be undertaken where higher risks are present.
- 4.6 CBs must ensure the AML/CFT/CPF risk management practices enable them to monitor transactions and to identify trends and anomalies. Where necessary, the CB should request further information to gain assurance about the nature of the transactions and parties to the transactions to satisfy itself of the level of ML/TF/PF risk exposure to such activity.
- 4.7 When trigger events or risk factors emerge in an existing CBR, the CB should review the relationship and apply the requisite due diligence to mitigate and manage the risk posed by the CBR, in line with its risk appetite.
- 4.8 Senior management should also be aware of the roles and responsibilities of the different services within the bank (e.g., business lines, compliance officers (including the chief or group AML/CFT officer, audit, or any other relevant stakeholder) pertaining to correspondent banking activities.

5 Compliance with SARB EFT Directive 01 of 2015 and FATF Recommendation 16

- 5.1 RBs should ensure that full and accurate originator and beneficiary information is included in payment messages sent to CBs, in accordance with FATF Recommendation 16 and to enable CBs to screen sanctions and monitor transactions.
- 5.2 If a CB decides to allow correspondent accounts to be used directly by third parties, it should conduct enhanced monitoring of these activities in line with the specific risks assessed.

⁷ The term payable-through accounts refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

5.3 Additionally, CBs should take adequate measures to prevent the processing of payments whereby the information embedded in the payment messages has been 'wire stripped'⁸ for the purpose of avoiding detection (e.g., sanctioned individuals or criminals).

5.4 CBs should ensure that when a RB's client cancels or recalls its payment to an intended beneficiary, that the funds are returned to the originator, unless the payment could be justified with supporting documentation.

6 Other considerations

6.1 The two common types of CBRs are vostro and nostro⁹ relationships, which both present risks and it is necessary for banks to identify all relevant factors that influence the risk rating of vostro and/or nostro accounts held with banks.

6.2 A 'one size fits all' approach is not aligned to or consistent with the spirit of a RBA. This stance is also reinforced by the FATF guidance which clarifies that, while additional CDD measures are required for cross-border correspondent banking, not all such correspondent banking services carry the same level of ML/FT risks. Cross border CBRs involving the execution of third-party payments should be considered as higher risk CBRs.¹⁰

6.3 There are certain basic principles to be guided by in terms of CBRs which should be included within the RMCP of a bank, i.e., for example, dealing with the lifespan of the CBR, from onboarding to off boarding of the same.

6.4 The RB should have a satisfactory level of ML/TF risk management processes and control measures which do not pass on undue risk to the CB who effects the cross-border payments.

6.5 Due to the nature of CBRs, it is useful for CBs to be aware of failures or deficiencies that have been highlighted globally over the years, to understand what led to deficiencies identified and thus introduce measures adequate to prevent similar non-compliance or deficiencies¹¹.

7 Nested relationships¹²

7.1 Nested relationships pose higher ML/TF risks to financial institutions and consequently banks should implement measures commensurately.

7.2 Nested CBRs may be an integral and legitimate part of correspondent banking. Effecting transactions via this method of processing payments may assist small local banks within the respondent's region to obtain access to the international financial system or to facilitate transactions where no direct relationship exists between the local banks and a foreign CB.

⁸ The practice of removing information from wire transfer messages so that the identity of potentially sanctioned countries, entities or individuals is hidden

⁹ A nostro account is one whereby a bank holds an account in a foreign currency at another bank. A vostro account is one whereby a bank holds an account for a foreign bank to enable the processing of payments of clients of the foreign bank in a differing currency.

¹⁰ See FATF, Guidance on correspondent banking services, October 2016, paragraph 13a.

¹¹ Source: <https://www.reuters.com/article/us-hsbc-probe-idUSBRE8BA05M20121211>, <https://www.occrp.org/en/daily/12710-deutsche-bank-fined-for-dealing-with-epstein-and-money-laundering-banks>, <https://www.reuters.com/article/us-lebanesebank-settlement-idUSBRE95O17P20130625>, <https://www.moneylaunderingnews.com/2020/06/westpacs-alleged-aml-failures-back-in-the-news/>

¹² Nested, or downstream accounts refer to the correspondent banking accounts used by other banks, through their relationship with the respondent bank, to conduct transactions and obtain access to other financial services via the correspondent bank.

- 7.3 The assessment of the ML/TF/PF risks associated with a nested relationship requires that CBs understand the purpose of the nested relationship. To this end they may inter alia consider the following factors:
- 7.3.1 the number and type of financial institutions a RB intends to provide a service to;
 - 7.3.2 whether the nested banks are located in the same jurisdiction as the respondent (considering the knowledge a RB might have of its own jurisdiction) or a different country;
 - 7.3.3 whether the jurisdiction of the nested bank and the areas the nested bank serves have adequate AML/CFT policies and implementation thereof; and
 - 7.3.4 the types of services the respondent offers to nested banks (proprietary only or client services such as CB).

8 Payable-through accounts¹³

- 8.1 Similar to nested relationships, PTAs present heightened ML/TF risks to nested relationships. CBs should ensure that they conduct adequate due diligence on their clients with direct access to correspondent accounts and that the RB can provide relevant CDD information upon request. In addition, they should ensure that the relevant senior management approvals are obtained prior to establishing a business relationship with the RB.
- 8.2 Questions similar to those referred to in the nested relationship section will assist CBs in creating and building a profile of the RB that it seeks to enter into a CBR with. Furthermore, it will assist the CB to identify, assess and rate the ML/TF risks that the RBs present and thus be in a position to apply a RBA in mitigating and monitoring those risks accordingly. The level of risk presented by a RB will determine the degree and frequency of due diligence to be undertaken in respect of the entity.
- 8.3 It is important that where there is a group structure with subsidiaries that have separate CBRs with the same CB, that the CB conducts due diligence on the individual RB subsidiary.¹⁴

9 Terminology

| Term | Definition |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nostro account | A nostro account is one whereby a bank holds an account in a foreign currency at another bank. |
| Vostro account | A vostro account is one whereby a bank holds an account for a foreign bank to enable the processing of payments of clients of the foreign bank in a differing currency. |

¹³ Payable through accounts are correspondent banking arrangements where, the respondent bank's clients are permitted to conduct their own transactions directly with the correspondent bank, through the respondent bank's correspondent account, without first passing through the respondent bank.

¹⁴ Para 38 and 39 <https://www.bis.org/bcbs/publ/d505.pdf> - Sound Management of Risks related to money laundering and financing of terrorism para 38 and 39

| Term | Definition |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Correspondent banking | Correspondent banking is the provision of banking services by one bank (the “correspondent bank”) to another bank (the “respondent bank”). 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. (FATF definition) |
| Shell bank | Shell bank means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence (FATF definition). |
| Payable through account | The term payable-through accounts refers to correspondent accounts that are used directly by third parties to transact business on their own behalf. (FATF definition). |
| Respondent bank | Bank that is the recipient of banking services of the correspondent bank. |
| Correspondent bank | Bank that provides the banking services to another bank. |
| Risk-based approach | A risk-based approach means that countries, competent authorities, and banks identify, assess, and understand the money laundering and terrorist financing risk to which they are exposed, and take the appropriate mitigation measures in accordance with the level of risk (FATF) ¹⁵ |
| Trigger event | In the context of correspondent banking, it is an instance/event which prompts a bank to take further action regarding a correspondent banking relationship e.g. review aspects of the due diligence, enquire further etc. |

¹⁵ <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/risk-based-approach-banking-sector.html>

10 Acknowledgement of receipt

- 10.1 Kindly ensure that a copy of this guidance note is made available to your institution's independent auditors. The attached acknowledgement of receipt, duly completed and signed by both the Chief Executive Officer of the institution and the said auditors, should be returned to the PA at the earliest convenience of the aforementioned signatories.

Fundi Tshazibana
Chief Executive Officer

Date:

The previous guidance note issued was Banks Act Guidance note 6/2022, dated 15 June 2022.