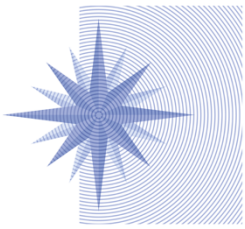

Banco Santander
Bank of America
Barclays
Citigroup
Credit Suisse
Deutsche Bank
Goldman Sachs
HSBC
JPMorganChase
MUFG Bank
Société Générale
Standard Chartered Bank
UBS

the Wolfsberg Group

Wolfsberg Financial Crime Principles for Correspondent Banking

1. Preamble

The Wolfsberg Group (the Group) has agreed that these Principles constitute global guidance on the establishment and maintenance of cross-border Correspondent Banking relationships. Institutions (for the purpose of this document, "Institution" will refer to the entity providing the services) should assess the applicability of these Principles to Domestic Correspondent Relationships, which may present a lower level of risk.

The Group believes that adherence to these Principles will promote effective risk management and enable Institutions to exercise sound business judgement with respect to their correspondent banking customers. Furthermore, adherence to these Principles will support the aim of Group members and the wider industry to prevent the use of global networks for criminal purposes.

This document is an update to the 2014 Wolfsberg Anti-Money Laundering Principles for Correspondent Banking and 2014 Correspondent Banking Principles FAQ documents, which have been retired.

For the purpose of this document, a financial crime compliance (FCC) programme includes, but is not limited to, measures under anti-money laundering (AML), counter-terrorist financing (CTF), anti-bribery and corruption (ABC), fraud and evasion of sanctions.

2. Correspondent Banking

A **Correspondent Relationship** is a business relationship provided by a financial institution (FI) for another Bank for the provision of commercial or business products or services. The degree of risk in a Correspondent Relationship is dependent on the risks posed by the nature of the relationship. For example, the degree of risk is generally higher where the bank receiving the services (Respondent) uses its Correspondent Relationship to provide banking services to its own customers. This is because the FI providing the services (Correspondent) is acting as an intermediary for underlying customers of another Bank. This activity may warrant a higher level of due diligence compared to when a Bank deals with another Bank on a purely principal to principal basis.

For the purpose of these Principles, **Correspondent Banking activity** (and by extension a Correspondent Banking Relationship) is defined specifically as the provision of banking-related services by one Bank to another Bank, for the execution of third-party payments, trade transactions and processing of paper clearing needs in a particular currency. These services may include provision of a current or other liability account and related services. A Correspondent bank enables its Respondent customers to provide their own customers with cross-border products and services. The Correspondent is effectively acting as the Respondent's agent or conduit, executing payments or other transactions for the Respondent's customers. These customers may be individuals, legal entities, or FIs.

The scope of such a relationship and the 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. A Correspondent Banking Relationship is characterised by its on-going, repetitive nature and does not generally exist in the context of one-off transactions.

These Principles extend to all Correspondent Banking Relationships which an FI establishes or maintains for another Respondent, including those where the Respondent is a branch, subsidiary, or affiliate of that Institution.

Institutions should also be mindful that some jurisdictions define Correspondent Banking in terms that are broader than what is generally considered to be Correspondent Banking activity. Accordingly, these Principles shall be implemented in a manner that is consistent with any applicable local requirements.

Although these Principles address the relationships maintained with other Banks, Institutions may decide, on a risk-based approach, to extend them to all the Correspondent Relationships which they maintain for Non-Bank Financial Institutions (NBFIs) and Payment Service Providers (PSPs), including but not limited to, Money Services Businesses (MSBs) / Money or Value Transfer Services (MVTS), financial technology companies (FinTechs), Virtual Asset Service Providers (VASPs) and new payment method (NPM) companies. Such Correspondent Relationships may be facilitating transactions that represent the same or greater risk and Institutions should determine whether to apply these principles to those relationships.

3. Responsibility and Oversight

Institutions shall define policies and procedures which require specified personnel to be responsible for ensuring compliance with their Correspondent Banking activities, including these Principles, and ensure such personnel have relevant experience and have undergone training on the risks involved in Correspondent Banking. A formal governance body with specific oversight of Correspondent Banking, inclusive of on-boarding, monitoring, and escalations, should be considered for this purpose. The governance body should include representation from the first and second lines of defence. The policies and procedures also shall provide for independent review by appropriate personnel to ensure continued compliance.

An Institution shall define an acceptable risk appetite which has been approved by their Board or other similar senior stakeholders. The risk appetite of the Correspondent Bank should set out the different types of parties and transactional activity the Correspondent prohibits or limits from being processed through its Respondents' account(s) and this should be communicated internally and to its Respondent customers.

4. Risk Based Due Diligence Guidelines / Considerations

All Respondent customers shall be subjected to appropriate due diligence that will seek to satisfy an Institution that it is comfortable conducting business with a particular Respondent, given the Respondent's risk profile and the nature of the business relationship with that Respondent. It may be appropriate for an Institution to consider, but not rely on solely, the fact that a Respondent operates in, or is subjected to, a regulatory environment which is recognised internationally as adequate in the fight against financial crime. The regulatory environment must be assessed in conjunction with other information obtained related to the specific Respondent. In these instances, an Institution may also rely on publicly available information obtained either from the Respondent or reliable third parties (regulators, exchanges, shared utilities, Wolfsberg Correspondent Bank Due Diligence Questionnaire (CBDDQ), etc.) to satisfy its due diligence requirements. The evaluation of risk and level of due diligence must consider the particular risk of the Respondent, be it the parent entity, subsidiary or branch of that parent, or an entity affiliated with the Institution itself and the potential financial crime risk associated with services provided to the customer. The Institution's policies and procedures shall require that the Respondent's information be reviewed and updated on a defined risk based, periodic basis. In addition, a trigger event, e.g. relevant financial crime-related adverse media, adverse customer behaviour or escalations related to unusual activity, which results in a material change in the risk profile of the Respondent, shall prompt a re-evaluation of the relationship.

In conducting due diligence on any Respondent Bank, the elements set out below to address specific risk indicators shall be considered, as appropriate:

- **The Respondent Bank's Geographic Risk**
  Certain jurisdictions are recognised internationally as having inadequate financial crime standards or insufficient regulatory supervision, thus presenting greater risk for financial crime, including corruption, terrorist financing, fraud, tax evasion or pose elevated risk of sanctions evasion. Jurisdictions with more robust regulatory environments represent lower risks. The effectiveness of the particular supervisory regime must be considered, particularly if the regime has been found to be deficient in its application of global financial crime standards. Institutions shall review pronouncements from regulatory agencies and applicable international bodies,

such as the Financial Action Task Force (FATF), to evaluate the degree of risk presented by the jurisdiction in which the Respondent is based, jurisdiction in which its ultimate parent is headquartered, and jurisdictions of those with whom they conduct business. In some cases, a sub-region of a country may be found to have specific risks that should be considered in assessing the Respondent's geographic risk.

- **Providing Correspondent Banking Relationships to your own Branches, Subsidiaries and Affiliates**
  When an entity affiliated with the Institution is the account holder, it is also a Respondent which is generally subject to the due diligence measures outlined in these Principles. The level and scope of due diligence on such a Respondent shall be dependent upon the level of control exercised by your parent Institution, certain facts unique to that branch, subsidiary, or affiliate, as well as regulatory standards and risks that may apply within the jurisdiction of that entity. Similarly, to the way branches, subsidiaries and affiliates as Respondents are assessed, an FI should consider factors that may be unique to its own affiliated entities, branches or subsidiaries which may dictate the level of enhanced due diligence (EDD) to be performed.

- **Providing Correspondent Banking Relationships to Branches, Subsidiaries and Affiliates of other Financial Groups**
  The determination of the level and scope of due diligence that is required on a Respondent shall be made after considering the relationship between the Respondent and its ultimate parent (if any). In general, in situations involving branches, subsidiaries or affiliates, when the parent is also a Respondent, the FCC programme of the Respondent Bank parent and extent of oversight of the branch, subsidiary and/or affiliate by the Respondent Bank parent in determining compliance with that FCC programme shall be considered in determining the extent of required due diligence on those entities. In instances when the Respondent Bank is a branch, subsidiary or affiliate, the entity shall be reviewed to determine if it has a comparable programme. However, certain facts unique to the branch, subsidiary or affiliate may dictate the level of EDD to be performed, particularly with respect to local, product or regulatory standards within the specific jurisdiction as well as any unique factors such as customer base or a branch operating under an offshore banking license.

- **The Respondent Bank Ownership and Management Structures**
  The ownership and management structure of the Respondent may present increased risks. Relevant risk considerations include the domicile and reputation of the owners; the corporate legal form of the Respondent; whether it is state-owned, publicly-held, or privately-owned; the transparency of the ownership structure and whether its shares are traded on an exchange in a jurisdiction with an adequately recognised regulatory regime. The structure and experience of Executive Management, e.g. most senior executives in charge of its day-to-day business, may also be appropriate for consideration given their influence and control over the Respondent. Depending on the circumstances of the Respondent, this may include the members of the Respondent's Board of Directors, Supervisory Board, Executive Committee, or its equivalent. The presence of any politically exposed persons (PEPs) in the Executive Management or ownership structure is also an important consideration, particularly in circumstances where the PEPs have day to day control over the Respondent. For all significant controlling interests, the ultimate beneficial owners, sources of wealth and background, including their reputation in the

marketplace (particularly as they may be related to any negative or adverse financial crime matters) as well as recent material ownership changes, shall also be ascertained to the extent available through inquiry or public sources. Similarly, a more detailed understanding of the reputation of the customer's Executive Management, as well as recent material changes in the Executive Management structure and the identity of any significant controlling individual(s), shall be considered where there is evidence of any associated adverse reputational risk.

- **Products and Services Offered by the Respondent**
  The types of financial products and services the Respondent offers to its own customers, as well as the type of markets the Respondent serves, may present greater risks. Involvement in certain higher-risk business segments and providing certain products or services generally recognised as being vulnerable to money laundering, corruption, terrorist financing or evading sanctions, may present additional risks and shall be considered in conjunction with the Respondent's controls to address such risks. Increased risk factors include provision of cross-border payment transactions, products offered to non-customers, products which involve the movement of physical currency or products offered that do not provide full transparency into the payment flows.

- **The Respondent Bank's Customer Base**
  The types of customers serviced by the Respondent may be relevant to the risk it poses to the Correspondent Bank. A Respondent that derives a substantial part of its business income from customers posing elevated risk due to the nature of their business, or jurisdictions in which they operate, may present greater risk themselves. Each Institution offering Correspondent Banking activity shall assess these factors and the Respondent's associated controls and determine whether this activity is within its risk appetite. Any potential activity outside the Institution's risk appetite should be communicated to the Respondent Bank.

- **Products or Services Offered to the Respondent Bank**
  The nature of the products and services offered to the Respondent can impact the risk associated with the relationship. Certain products are more vulnerable to financial crime and in offering those the Institution should consider all relevant risk factors, including their own ability to monitor the transactions for unusual activity. The business purpose(s) for the relationship with the Respondent as well as expected activity for the products and services offered should be documented and evaluated for reasonability and referred to during the life of the relationship to assist in identifying activity that is inconsistent with the documented expectations.

- **Regulatory Status and History**
  Reasonable measures shall be taken to verify that the Respondent is subject to regulatory oversight and is duly licensed in the jurisdiction(s) where it operates. The Institution shall determine if the Respondent has been the subject of any relevant, material regulatory action and assess the extent to which it is relevant to the establishment/continuance of the relationship or whether enhanced risk mitigation measures may be appropriate.

- **Financial Crime Controls**
  Using a risk-based approach, the Institution shall evaluate the quality of the Respondent's FCC programme, including how it meets internationally recognised standards and how sufficiently it

mitigates the risk presented based upon their products, customer base and jurisdiction. The extent to which an Institution will enquire about the FCC programme will depend upon the risks presented. If appropriate, the Institution should speak with representatives of the Respondent to obtain additional information, review FCC controls and corroborate findings.

- **No Business Arrangements with Shell Banks**
  The Institution shall confirm that the Respondent is not a Shell Bank[1] and does not provide products or services to Shell banks.

- **Customer Visit**
  Unless other measures suffice, a representative of the Institution should visit the Respondent Bank at their premises, prior to or within a reasonable period of time after establishing a relationship with a Respondent, to support the customer due diligence process. Site visits by financial crime subject-matter experts may also be conducted if deemed necessary. Institutions should make risk-based decisions on measures to take if a customer visit is not possible.

The Group has developed a CBDDQ which should be used to collect the related customer due diligence information. The Group has also published extensive guidance materials on the CBDDQ.

5. Enhanced Due Diligence

In addition to due diligence, each Institution shall also apply enhanced due diligence (EDD) to those Respondents which present greater risks. The EDD process shall involve further consideration of the following elements, designed to satisfy the Institution that it has secured a greater level of understanding:

- **PEP Involvement**
  If a PEP appears to have involvement in the Respondent, the Institution shall ensure it has an understanding of the person, their role and the appropriateness of that role, their ability to influence the customer and the risk they may present to the relationship.

- **Downstream FIs**
  A downstream FI (also referred to as "nested") arrangement occurs when a Respondent provides Correspondent Banking services to other FIs, domiciled inside or outside the Respondent's country, to facilitate products and services on behalf of the downstream FI's customers, e.g. when a regional savings bank offers correspondent services to local savings banks in its area. Through correspondent banking relationships, FIs can access financial services in different jurisdictions and provide cross-border payment services to their customers, supporting international trade and financial inclusion.

  When these services are offered by a Respondent to a downstream FI, the Institution (Correspondent) shall take reasonable steps to understand the types of FIs to whom the Respondent offers the downstream correspondent services. These steps may include consideration of the types, scale of services and geographic location of downstream FI(s) and their customers, and any identified issues with either the Respondent or its downstream FI's

[1] As defined in the FATF Recommendations Glossary, a Shell bank is "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 a meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence."

customers. The Institution should also consider the degree to which the Respondent examines the Financial Crime controls of the FIs to which it offers those services and determine if controls are in place to ensure payment transparency.

- **Approval**
  Approval of higher-risk Correspondent Banking relationships at the time of on-boarding shall be subject to a higher level of approvals by the first line of defence and the relationship shall be reviewed periodically.

6. Monitoring and Reporting of Suspicious Activities

The Institution shall implement policies and procedures to detect and investigate unusual or suspicious activity and report any such activity as required by applicable law. Such policies and procedures should include guidance on what is considered to be unusual or suspicious and give examples thereof. The policies and procedures shall require appropriate monitoring of the Respondent's activity, incorporating due diligence results, such as customer risk rating and other factors considered meaningful in the assessment of transaction activity. In turn, the results of suspicious activity monitoring shall be factored into the periodic review of the customer relationship, particularly when the results of transaction monitoring indicate elevated risk levels. The relationship between due diligence information and transaction monitoring shall be continuous throughout the life of the Respondent relationship and apply to both the Respondent and any related "suspect" activity. This is commonly referred to as the feedback loop.

7. Ongoing Review of Correspondent Banking Relationships

Institutions shall review the relationship with the Respondent on an ongoing basis to assess whether the relationship remains within the risk appetite. This review should include measuring the effectiveness of the Respondent's FCC programme on a risk-based approach and seek to determine whether the Respondent is able to demonstrate that its FCC programme is commensurate to the nature, scale, size, and complexity of its business. The risk-based review to determine effectiveness of the Respondent's FCC programme should include assessing the Respondent's own ability to manage and detect financial crime risks within the transactional activity of its underlying customers. This review should leverage all information available at the time to assess whether the relationship should be maintained. Some examples of information that may be leveraged are: the existence and nature of suspicious activity reports filed on both the Respondent and its underlying customers, material adverse media, activity that is not consistent with due diligence information or expected activity, material/unexplained changes in volume and/or value of transactions, non-compliance with payment transparency rules, sanctions metrics, and non-response or inadequate response to request(s) for information. Comparison between what the Respondent stated about its FCC programme at onboarding/the last periodic review and how that programme is observed in practice should also be considered.

8. Integration with Financial Crime Compliance Programme

These Principles shall form an integral component of the institution's wider FCC programme, including controls against bribery and corruption, fraud and evasion of sanctions.

Wolfsberg Frequently Asked Questions (FAQs) on Correspondent Banking

To provide continuing guidance on Financial Crime controls in relation to Correspondent Banking, the Group has prepared these FAQs, based on the Group's views on current best practices and, in some respects, on how the Group believes those practices should develop over time.

1. Why is there so much regulatory and law enforcement scrutiny of Correspondent Banking?

Regulators and law enforcement continue to scrutinise due diligence and risk management practices in the Correspondent Banking arena due to the inherent risks associated with processing transactions for other FIs and their customers, as well as the documented cases in which Correspondent Banking accounts have been used to move illicit funds.

The inter-relationships built up over decades between institutions within Correspondent Banking networks have produced a mechanism which is of fundamental importance to the global economy. This mechanism facilitates the movement of money from one person or entity to another, and from one country to another, as well as currency conversion. The efficiency of this important mechanism may also unintentionally facilitate the activities of those who seek to launder the proceeds of financial crime or to finance terrorism and other unlawful activities. Law enforcement and regulatory actions have resulted in significant financial penalties and have highlighted the vulnerabilities to which FIs are exposed when there are failures in the risk management framework, particularly in the areas of governance, customer due diligence, risk assessment and transaction monitoring. Correspondent Bank accounts have been used to move the proceeds of illicit and evasion of sanctions. This misuse of the financial system highlights the need for proactive vigilance in maintaining an effective FCC programme for Correspondent Banking and will mean there is a continued heavy focus by regulators and law enforcement.

As noted in the Principles, in dealing with Respondents, a Bank (referred to in these FAQs as the "Institution") is acting as its Respondent's agent or conduit, executing payments or other transactions for the Respondent's customers. These customers may be individuals, legal entities or even other FIs, and the beneficiaries of the transactions may be customers of the Institution or customers of other FIs.

The Institution typically has no direct relationship with the underlying parties to any transaction routed through it and will not be in a position to verify identity or to understand fully the nature of the specific transaction, particularly when processing electronic payments (wire transfers) or clearing cheques.

2. Do these Principles apply if a Respondent is a branch, affiliate, or subsidiary of an existing Respondent customer?

Yes. The risk factors that are applied to a Respondent need to be applied equally to their branches, affiliates and subsidiaries when they are direct customers. While it may be possible to be informed by the FCC programme of the Head Office, those entities may possess their own unique customer, product and geographic risks which must be considered. For example, a particular branch may target a high-risk customer segment or offer higher-risk products, may operate in a jurisdiction that is higher-risk for corruption and money laundering, may have been the subject of material negative media in relation to its financial crime compliance programme and/or be operating under an offshore banking license.

Additionally, the structure and execution of a particular subsidiary’s FCC programme may be impacted by local regulatory requirements and may vary based on the level of control and oversight exercised by the

parent bank. For example, subsidiaries not wholly owned by the Respondent parent may have other controlling owners and may operate under different FCC standards. The net result is that the financial crime risk of a branch, affiliate or subsidiary may differ from the overall assessed risks of the parent.

Regulations in some jurisdictions set standards for customer due diligence – Correspondent Banking or otherwise – and treat each distinct account holder as a customer for purposes of compliance with applicable requirements. To the extent that branches, affiliates, and subsidiaries maintain their own accounts with the Institution, they may be subject to the regulatory requirements applicable to all account holders/customers.

3. Should the Institution offering the Correspondent Banking services treat its own branches, subsidiaries and affiliates as distinct customers subject to the Principles?

Yes. The inherent risks of Correspondent Banking relationship do not differ when the service is offered to one's own branches, subsidiaries, and affiliates. The level and scope of due diligence on such a customer shall be dependent upon the level of control exercised by the Institution's parent.

An Institution's branches, subsidiaries and affiliates may engage in business with customer types that pose varying levels of risk, and the branch/subsidiary/affiliate may operate in a jurisdiction that is higher-risk for money laundering and corruption. Other risks to consider include the presence of additional controlling owners, differences in application of the Institution's FCC programme and the existence of adverse information about the customer's FCC controls. Adverse information, when considered in the context of an affiliated entity, may not be limited to information that exists in the public domain, as the Institution may be in possession of internal information such as the results of internal audits or regulatory examinations which indicates that there is potentially heightened risk associated with a particular branch, subsidiary or affiliate receiving Correspondent Banking services.

Institutions providing Correspondent Banking Relationships to branches, subsidiaries and affiliates should ensure that their FCC programme is designed to assess the risks of the customer, using all relevant risk measures available within the Institution and that appropriate levels of transaction monitoring and reporting of suspicious activity are in place.

4. Should Euro clearing relationships with European Union (EU) member banks be treated as Foreign Correspondent Banking relationships under the Principles?

Yes, when an EU-based Institution provides Euro-clearing services to other institutions within the EU, the Institution should treat these customers as Foreign Correspondent Banking relationships. While these institutions share the same currency, they operate within different sovereign nations that may pose specific geographic risks. Additionally, notwithstanding the EU AML Directive(s), country-specific regulation and the strength of AML enforcement regimes may vary between EU member countries. For these reasons, Institutions need to ensure they apply the Principles to Correspondent Banking relationships with other EU member institutions.

5. Should relationships with higher-risk Respondents be avoided completely?

It is not within the scope of the Group's work to advocate a general avoidance policy with respect to relationships with higher-risk Respondents. Each Institution should assess their Respondents within the context of its own risk parameters and its ability to manage the risk. When higher risks are identified, an

Institution may decide, working with the Respondent, whether they can mitigate the risk to an acceptable level which may include limiting certain transactions.

There are some relationships that should be avoided. These include relationships with:

- Shell banks – Institutions should also exercise care to ensure that they do not knowingly deal with FIs which themselves deal with shell banks;
- Unlicensed and/or unregulated banks or NBFIs;
- Any Respondent where the results from conducting due diligence produce significant concerns that cannot be resolved; and
- Situations where the Respondent's FCC controls are considered inappropriate and/or insufficient and the Respondent does not satisfy the Institution that necessary remedial action will be undertaken.

6. What is a payable-through account and why are they considered high-risk?

The FATF recommendations define the term payable-through accounts as correspondent accounts that are used directly by third parties to transact business on their own behalf.[2] In other words, the institution providing the Correspondent Banking services allows its Respondent's accounts to be accessed directly by the customers of that Respondent, e.g. the customers of the Respondent may have cheque writing privileges or otherwise be able to provide transaction instructions directly to the Institution. This is different than a traditional Correspondent Banking relationship in which the Respondent is executing transactions on behalf of its customers.

The arrangements pose greater risk to an Institution if it does not have access to information about the third parties accessing the account.

7. What is the purpose of the Wolfsberg Correspondent Bank Due Diligence Questionnaire?

The Wolfsberg CBDDQ has been designed to provide a reasonable and enhanced view of a FI's FCC policies and practices. The CBDDQ covers a Respondent's control environment to allow Institutions to obtain a greater level of understanding of the cross-border and/or other higher-risk Correspondent Banking relationship they are entering into and/or continuing.

Institutions should use the CBDDQ as part of their FCC programme's due diligence requirements for a particular Respondent, however, Institutions are responsible for ensuring their FCC programmes are designed to meet regulatory requirements/expectations and internal risk management standards, thereby determining the exact manner in which the Questionnaires are utilised in their FCC programmes.

Detailed guidance on the Questionnaire is available on the Wolfsberg website.

8. What should the Institution expect from the Respondent?

The Institution should set expectations of the Respondent, including:

- Partnership – clear and open communication related to FCC matters and the provision of complete and accurate due diligence information;

[2] Definition from FATF, Interpretive Notes to Recommendation 13, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION, The FATF Recommendations.

- Responses to Requests for Information – timely and fulsome responses to inquiries related to transactions in the account; and
- Understanding of the Institutions' risk appetite and compliance with any restrictions communicated.

The Institution should assess the level of compliance with these expectations on an ongoing basis (e.g. as part of but not limited to periodic reviews).