COMMISSION FOR THE PREVENTION OF MONEY LAUNDERING AND MONETARY OFFENCES

GUIDANCE FOR REGULATED ENTITIES

June 2019

BANKING ON BANKING CORRESPONDENCE

CONTENTS

I. Introduction. 2

II. Purpose and target audience. 4

III. Concepts and types of relationships: the framework of Law 10/2010 of 28 April. 5

IV. Due diligence in correspondent banking relationships. 7

IV.1 Assessment of the risks associated with the business relationship. 7

IV.2 Due diligence applicable at the start of the business relationship. 10

IV.3 Risk management during the course of the business relationship. 12

IV.4 Documentation of compliance with the obligation to apply enhanced due diligence measures. 17

V. Some considerations regarding the provision of banking services to payment institutions. 18

Annex 1. Illustrative list of high-risk transactions in correspondent banking relationships. 19

Annex 2. Risk factors in correspondent banking relationships as set out in the European Banking Authority's Guidelines on risk factors, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority, dated June 2018. 21

GUIDANCE ON THE APPLICATION OF MEASURES FOR ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM (AML/CFT) IN BANKING CORRESPONDENT RELATIONSHIPS

I. INTRODUCTION

Correspondent banking relationships are a fundamental element underpinning the functioning of the financial system and the global interconnection of the economies of different countries.

The need for correspondent banking arises when a financial institution needs to provide a service in a third country where it has no physical presence or, even if it does have a physical presence, where it does not have access to the payment system for that country's currency. To this end, it contacts a financial institution in that country and reaches an agreement to exchange RMA (Relationships Management Application) codes[1] and, usually, to open an account (nostro/vostro account). This network of international agreements has shaped the current correspondent banking system, which is essential for the swift and effective operation of payment systems. Over recent decades, financial institutions around the world have developed an international payment system that enables financial transactions to be processed reliably, quickly and efficiently. The smooth functioning of the international payment system is essential for ensuring global financial stability.

However, the correspondent banking network is a channel that can be used for Money Laundering and Terrorist Financing. Given the ease and speed with which large sums can be moved through complex financial transactions, international payment systems allow funds to be severed from their criminal origin, making it virtually impossible to trace them. This difficulty is compounded by the fact that the banks involved in the payment chain are subject to the regulations of the country in which they are based.

Similarly, payment institutions process transfers globally through the use of correspondent institutions in third countries, thereby replicating many of the risks associated with traditional correspondent banking.

The same applies to securities markets, which are characterised by their complexity, international nature, high volumes of assets under management, the speed of transactions, a high level of intermediation and anonymity. These characteristics, furthermore

[1] A messaging function that enables SWIFT members to exchange messages via this network. The use of RMA is mandatory for sending and receiving any SWIFT message, with certain exceptions that do not apply to transfers or payments made by customers or financial institutions.

Whilst they contribute to economic growth, they also create opportunities for Money Laundering and Terrorist Financing schemes, which must be properly countered.

For all these reasons, correspondent banking relationships in these sectors require the implementation of specific and additional preventive measures, over and above those traditionally set out in the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) policy for application to the end customers of financial institutions.

In Spain, the regulation of correspondent banking relationships is set out in Law 10/2010 of 28 April, which deals with Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) (hereinafter 'Law 10/2010 of 28 April'); specifically, in Article 13, which was recently amended by Royal Decree-Law 11/2018 of 31 August.

The importance of implementing appropriate measures to prevent Money Laundering and Countering the Financing of Terrorism (AML/CFT) in correspondent banking relationships – particularly those relating to the monitoring of transactions – has once again been highlighted by recent cases involving credit institutions in the European Union which, due to shortcomings in this area, have seen their stability and reputation affected.

For all these reasons, it is necessary to supplement this regulation with guidance that improves the practical application of the provisions contained in the Law, by clarifying the regulators' expectations. In drawing up this document, the following documents have been taken into account, in addition to the legislation currently in force in Spain:

- "Guidelines on risk factors", issued by the European Supervisory Authorities, 26 June 2017.
- "Guidance on the Prevention of Money Laundering Risks in Correspondent Banking" by the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences (SEPBLAC), December 2007.
- "Guidelines on Correspondent Banking Services" adopted by the FATF, October 2016.

Other relevant documents in this regard

- "Sound management of risks related to money laundering and terrorist financing", Basel Committee on Banking Supervision, July 2017.
- "Correspondent banking", Committee on Payments and Market Infrastructures, July 2016.

II. PURPOSE AND TARGET AUDIENCE

The purpose of these guidelines is to clarify the scope of the obligations that financial institutions must fulfil in their cross-border correspondent banking relationships, in accordance with Article 13 of Law 10/2010 of 28 April, and how these obligations interact with other rules and obligations contained in the legislation on Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT).

These guidelines are addressed to:

a) Credit institutions.

b) Payment institutions.

c) Financial institutions providing services similar to those of a correspondent bank in relation to securities, including the safekeeping and transfer of such assets.

III. CONCEPTS AND TYPES OF RELATIONSHIPS: THE FRAMEWORK OF LAW 10/2010 OF 28 APRIL.

Correspondent banking. A correspondent banking relationship is defined as the provision of banking services by one bank, acting as a correspondent, to another bank as a client (which is normally the holder of a vostro account), including, amongst others, current accounts or other liability accounts and related services, such as cash management, international fund transfers, cheque clearing, and foreign exchange services.

The concept of correspondent relationships covers any relationship between credit institutions and/or financial institutions that provide services similar to those of a correspondent to a customer, including, but not limited to, **relationships established for securities transactions or custody, or the management of transfers**. Consequently, the provisions of this guidance shall also apply to these other types of relationships.

Furthermore, SWIFT key exchange relationships (RMA) can create a situation similar to that of a traditional correspondent relationship due to the sequence of transactions exchanged, regardless of whether the transactions are settled by a correspondent or by a multilateral system (such as TARGET). Where the substantive relationship arising from the exchange of keys is equivalent to a traditional correspondent banking arrangement due to the repetitive and non-exceptional nature of the transactions, the measures described in this document shall apply.

Furthermore, cash accounts held with custodian banks by financial institutions and linked to securities accounts may be used for pure correspondent banking operations, such as receiving or making transfers on behalf of clients; these transactions do not therefore relate to securities trading. The measures described in this document shall also apply in such cases.

Nostro/Vostro account. An account held in the books of the institution providing correspondent banking services, used for the settlement of transactions. It is a single account with two distinct names: it is referred to as a 'nostro account' by the client institution and as a 'vostro account' by the institution providing the correspondent banking service.

SWIFT Key Exchange Relationships (RMA[2]). A messaging function that enables SWIFT members to exchange messages via this network. The use of RMA is mandatory for sending and receiving any SWIFT message, with certain exceptions that do not apply to transfers or payments made by customers or financial institutions.

Cross-border banking correspondent arrangements. This refers to the provision of correspondent services by an institution established in Spain to a client institution in a third country, whether or not that country is a member of the European Union.

Correspondent institution. This is an institution that processes or executes transactions on behalf of end customers. This institution has no direct relationship with the end customer to whom the services are provided. In addition to acting as an intermediary in the transfer of funds or securities on behalf of end customers, the correspondent bank may provide other types of services, such as those relating to trade finance, cash settlement, liquidity management, or the granting of short-term loans or investment in foreign exchange.

Client institution. This refers to the financial institution to which the correspondent institution provides services.

Accounts used for payments (PTA). This involves establishing or maintaining correspondent relationships which, either directly or through a sub-account, enable transactions to be carried out on behalf of the clients of the represented credit institution. Law 10/2010 of 28 April expressly prohibits this practice in Article 13.4.

Shell banks/institutions. This term refers to financial institutions that meet the following conditions:

(i) their business is conducted outside the jurisdiction in which they are authorised,

(ii) they do not usually have a physical presence in that jurisdiction, but merely a registered agent who is not involved in the day-to-day running of the business,

(iii) they do not keep records of transactions, and

(iv) is not subject to inspection by the banking authority that authorises it to conduct its business.

[2] RMA: Relationships Management Application. A messaging function that enables SWIFT members to exchange messages via this network. The use of RMA is mandatory for sending and receiving any SWIFT message, with certain exceptions that do not apply to transfers or payments made by customers or financial institutions.

IV. DUE DILIGENCE IN BANKING CORRESPONDENT RELATIONSHIPS

IV.1 Assessment of the risks associated with the business relationship.

When establishing correspondent banking relationships, it is necessary to comply with the general due diligence obligations set out in Articles 3 et seq. of Law 10/2010 of 28 April in relation to the client institution.

In principle, in the case of financial institutions – with the exception of payment institutions – established in the European Union or in equivalent third countries that are subject to supervision, in order to ensure compliance with obligations relating to Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT), simplified due diligence measures may be applied (Article 15 of the Regulations under Law 10/2010, approved by Royal Decree 304/2014 of 5 May, hereinafter 'the Regulations').

Simplified due diligence measures may, in accordance with Article 17 of the Regulation, consist of verifying the identity of the customer or the beneficial owner only when a quantitative threshold is exceeded after the business relationship has been established (it is important to note that what may be deferred is the verification of identity, not the identification itself), reducing the frequency of the document review process, reducing the monitoring of the business relationship and the scrutiny of transactions that do not exceed a quantitative threshold, and not collecting information on the customer's professional or business activity, inferring the purpose and nature from the type of transactions or business relationship established.

However, the possibility of applying simplified due diligence measures extends only to activities carried out in the client's own interest, where the Law provides for such a possibility (a public body, a financial institution, a listed company). In cases other than such activities carried out in the client's own interest, it cannot be said that there is a low risk of Money Laundering or Terrorist Financing that might justify the application of simplified due diligence measures.

Thus, Article 13 of Law 10/2010 of 28 April imposes enhanced due diligence measures in relation to cross-border correspondent banking, which in many cases reflects the activities undertaken by financial institutions to fulfil their clients' instructions and serve their interests.

However, it must be made clear that the correspondent is not deemed to be acting on behalf of the end customers; consequently, the correspondent institution is not required to be aware of or apply customer due diligence measures in respect of the client financial institution's end customers. As indicated below, it will only be necessary to know who those customers are in certain cases, not as a general rule.

Domestic banking relationships similar to correspondent banking. The higher inherent risk associated with cross-border correspondent banking relationships does not mean that there are no risks in relationships that may be established with domestic institutions. In such cases, whilst the regulation and supervision of the client institution will be the same as that of an institution providing a service equivalent to that of a correspondent, there may be differences in other respects, such as the quality of procedures or the type of products and services offered. These factors must be taken into account in the processes for determining risk and the measures to be applied to mitigate such risks, with the ongoing monitoring of these business relationships being a fundamental element. Consequently, in business relationships similar to correspondent banking, conducted in the domestic context, simplified due diligence measures do not apply; such measures are only applicable in cases where the client institution is, in fact, the end customer of the transaction carried out or service provided.

Risk levels in cross-border correspondent banking relationships. Not all types of cross-border correspondent banking relationships carry the same level of risk; therefore, in each case, the extent of the additional measures to be applied must be tailored to the circumstances and potential risks. It is therefore necessary for correspondent institutions to carry out a detailed and specific assessment of the client institution's risk level, taking into account all relevant risk factors. Consequently, the controls to be applied and the monitoring of business relationships will vary according to the inherent risk identified for each specific relationship, taking into account the prevailing circumstances.

Fact**ors for determining risk**. Factors to be taken into account when assessing the risks associated with correspondent banking could include, by way of example and without being exhaustive:

- the jurisdiction of the client institution;
- the quality and conditions of regulation and supervision in the client institution's country;

- the group to which the institution belongs and the jurisdictions in which the group's subsidiaries and branches are located;
- the management and ownership of the client organisation, including information on its beneficial ownership;
- the products and services they offer;
- its customer base;
- the services requested for the correspondent banking relationship;
- the quality of the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) procedures established by the institution in question.

Once again, it should be noted that this list is provided purely by way of example and cannot be regarded as an exhaustive list of controls to be applied in correspondent banking relationships; there may be other issues and factors to be considered in a specific case that are not included in the list above.

Information for carrying out the risk analysis. The information required to carry out this risk assessment may come from various sources; however, by way of example, the following documents and information may be cited as useful for assessing the organisation's level of risk:

- National risk analyses published by the country's competent authorities or by supranational bodies, such as the EU.
- The applicable regulations in the jurisdiction where the client organisation is located and how they are applied.
- A review of publicly available information on administrative or criminal sanctions imposed in that jurisdiction.
- Any other information published by the supervisory or regulatory authority in the relevant jurisdiction.
- Annual reports submitted by the entity to the stock exchange operator.
- Mutual evaluation reports on countries prepared by the FATF and FATF-style regional bodies.
- Other relevant reports produced by international organisations (Basel Committee on Banking Supervision, International Monetary Fund, World Bank).
- List of countries subject to the FATF review process.
- List of countries with strategic deficiencies, as identified by the European Commission.

- Information provided by the managers and those responsible for the client institution's Money Laundering policy.

IV.2. Due diligence applicable at the start of the business relationship

Identification. When establishing a business relationship, as a first step, the correspondent institution must identify and verify the identity of the client entity through a reliable and independent source. For example, it may be sufficient to obtain evidence of registration with the supervisory authority or the Commercial Register of the country of origin.

Beneficial owner. It must also identify and take reasonable steps to verify the identity of the beneficial owners, so that the correspondent institution can be certain that it knows who the people behind the entity are. Obviously, this process also involves understanding the ownership and control structure of the client entity, all with a view to clearly establishing that the client entity is not a shell bank.

Purpose and nature of the business relationship. Furthermore, the correspondent must gather sufficient information to understand the purpose and intended nature of the business relationship to be established; it is necessary to know which types of the institution's customers might benefit from the correspondent services provided, the expected level of activity, the volume and value of the transactions, and the type of transactions envisaged.

At this stage, the correspondent institution must gather sufficient information to understand the nature of the client institution's business; that is, to ascertain its target market and the customer segment it serves, the markets and countries in which it operates, the channels it uses and the services it provides, including the possible provision of *'nested' account* services. As part of this process, it must be verified that the client entity does not permit the use of its accounts by shell banks. This may include requiring the client entity to confirm that it does not permit the use of its accounts by shell banks, taking into account the relevant provisions of its policies and procedures or publicly available information, as well as the legal provisions in force in the country of establishment that prohibit the provision of services to shell banks.

Reputation. The correspondent institution must also gather sufficient information and assess, on the basis of information in the public domain, the reputation of the entity and

the quality of the supervision to which it is subject, including whether (and when) it has been the subject of an investigation.

Prevention system. The correspondent must assess the client institution's anti-money laundering controls and their quality; merely obtaining a copy of the institution's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) policy and procedure documents is not sufficient. The assessment must include confirmation that the client institution's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) systems are subject to an independent audit (which may be external or internal).

In business relationships where a higher level of risk has been identified, the assessment process should be more thorough and detailed, including, where appropriate, a review of the independent audit, interviews with compliance officers, a third-party review or even an *on-site* visit.

Documentation of each party's responsibilities. One way in which risks can be managed effectively is by clearly defining the respective obligations through the conclusion of a written agreement, regardless of the form in which this agreement is drawn up. The content of the agreement must include:

- the purpose of the correspondent banking relationships and their intended use, specifying the products and services to be provided;
- how the correspondent bank's infrastructure may be used (for example, whether it may be used by other credit institutions during their relationship with the client institution)
- the client institution's responsibilities regarding compliance with Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) requirements;
- the manner in which the correspondent institution will monitor the relationship to determine how effectively the client institution is applying customer due diligence measures and implementing preventive controls;
- any potential restrictions that the correspondent bank may wish to impose on the use of the correspondent account (for example, limiting the types of transactions, volumes, etc.);
- the client institution's obligation to provide, in all cases, information on specific transactions as may be required by the correspondent institution itself or at the request of its authorities;

- the conditions relating to the applications for information regarding specific transactions detected by the correspondent institution; and
- the circumstances and procedures for terminating or restricting a business relationship.

The level of detail and the content of the contract itself will vary depending on the circumstances, including the nature of the correspondent banking relationship and the level of risk. Where the risk associated with the relationship is high, it may be advisable for the correspondent to ensure that the client institution complies with the obligations undertaken under the agreement between them, for example, through post-transaction monitoring.

Authorisation by senior management. Furthermore, as provided for in Article 13.2(c) of Law 10/2010 of 28 April, decisions relating to cross-border correspondent banking must be taken at a senior level.

The senior manager granting authorisation shall not be the same person who initiates the relationship; the greater the risk associated with the relationship, the higher the rank of the senior manager approving it. Correspondent banks shall keep senior management informed of high-risk correspondent banking relationships and of the measures they take to manage that risk effectively.

In the case of financial groups whose parent company is based in Spain and which have a cross-border presence, the senior manager responsible for authorisation in Spain must, at the very least, endorse the decisions of their subsidiaries. Prior to such endorsement, it must be verified that the documentation, the contract and the risk assessment carried out by the subsidiary are, at the very least, as thorough and comprehensive as those followed in Spain by the parent company.

Verification of information. In addition to complying with these due diligence measures, the requirements for verifying the information requested must be met using reliable and independent sources, including, amongst others, commercial registers, registers of authorised entities maintained by the competent authorities, or registers of beneficial owners…

IV.3. Risk management in the conduct of business relationships.

Regular review of information on the client organisation. There must be a regular

review of the information initially obtained from the client organisation, to ensure that it remains up to date and in line with the risks associated with the business relationship. The intervals at which the information is reviewed will vary and will depend on the current risk; however, in the case of cross-border correspondent banking clients and domestic correspondent banking clients posing a higher-than-average risk, reviews will take place at least once a year.

Should these periodic reviews reveal any significant changes in the client institution, the correspondent institution must assess whether its risk profile needs to be adjusted, and to this end must obtain the information and documentation it deems necessary.

Monitoring of transactions. A fundamental part – perhaps the most important – of due diligence processes, including in the context of correspondent banking, is the monitoring of the business relationship. All due diligence measures implemented, however stringent they may be, may prove ineffective if they are not accompanied by adequate monitoring of the business relationship.

The monitoring process will cover all transactions carried out, both those conducted directly by the organisation (originating from or destined for the organisation) and those carried out through intermediaries. This means that suitable tools must be in place for this purpose, along with the necessary resources to ensure they are used effectively.

The primary aim of this monitoring will be to determine the extent to which the transactions carried out conform to the expected pattern and to detect changes in the transaction profile that may indicate a deviation from the intended use of correspondent banking services.

The mechanisms and approaches used to carry out monitoring will vary depending on the level of risk. This is not only based on the initial risk assessed at the time the business relationship is established, but must also take into account the specific development of the business relationship. In this regard, account will be taken, for example, of any failures to provide information, both that which must be submitted on a regular basis and that which may have been requested at a specific point in time. Furthermore, awareness of and monitoring of the types of messaging services used are considered fundamental, with a view to identifying inconsistencies in the expected conduct of the business relationship.

In any event, periodic reviews must be carried out on the basis of the risks identified, in accordance with pre-determined procedures and alert systems, which must be defined taking into account the nature of the

relationship, the services provided, the overall risk and the client organisation's behaviour throughout the life of the business relationship.

In addition to general monitoring of the relationship, selective monitoring systems will be developed based on specific risk factors, for example, the existence of suspicious activities or the detection of payment flows that are inconsistent with the stated purpose of the account.

For example, in the case of relationships whose main purpose is to process cross-border transfers on behalf of the client institution's customers, one of the aspects that must be monitored is the proper application of obligations relating to transfers[3] and financial sanctions[4] . In such cases, specific areas of interest could include information on the client institution's mechanisms for identifying transactions lacking the required information on the payer and the payee, its risk-based policies and procedures for determining how to handle such transactions, its sanctions screening systems, and its procedures and systems for resolving false positives.

Adapting mitigation measures to changing risks. Correspondent banking relationships are highly diverse in nature and, therefore, whilst categorised as high-risk business relationships, they may be associated with a wide range of risk levels. The level and nature of risk may fluctuate over the course of any relationship, and adjustments must be made to the correspondent institution's risk management strategy to reflect these changes. This is why ongoing monitoring, including periodic reviews, is important, so that the correspondent institution is aware when the level or nature of residual risk changes.

Request for information on specific transactions. Where the monitoring and control system detects a transaction that could indicate unusual activity, the correspondent bank must have internal processes in place to examine the transaction in greater detail. These processes may involve requesting information about the transaction from the client bank, in order to clarify the situation and, where appropriate, resolve the alert.

[3]Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, and FATF Recommendation 16.

[4] Sanctions adopted by United Nations Security Council Resolutions and applicable EU Regulations

In any event, requests for additional information should not be made on a mass scale, but should be limited to the transaction or transactions that triggered the alert, including, where applicable, information relating to an omnibus account.

The information requested will vary depending on the alert triggered and its risk level, and may include a request for access to information about the end customer. The aim is not to duplicate the due diligence process carried out by the client institution, but to obtain sufficient information to confirm that the transaction is reasonable. Examples of the information that may be requested include:

- Duration of client "X"'s relationship with the organisation;
- Risk rating assigned by the client organisation to client "X";
- Purpose of the account(s) held by client "X" (business, personal, other);
- Details of client "X"'s parent company and the name(s) of the beneficial owner(s);
- Source of client "X"'s funds;
- Consistency between client "X"'s transaction history and their due diligence data, or with any other information available to the bank;
- Justification for the transaction between customer "X" and the counterparty;
- Nature of the relationship between customer "X" and the counterparty;
- Possible affiliation of customer "X" with a third party;
- Further details regarding the goods/services being exchanged between customer "X" and the third party, which do not appear in the payment details but which may explain the transaction;
- Status of customer "X"'s bank account (open/closed).

Where, upon requesting information from the client institution regarding a specific transaction, no response is received in the manner or within the timeframes specified, the institution shall consider whether to reject the order and return it to the originating institution. It shall also assess the need to carry out a special review and, where appropriate, report the matter to SEPBLAC on the basis of suspicious activity and terminate the business relationship.

Failure to respond to requests for information regarding specific transactions will be taken into account when reassessing the risk associated with the correspondent banking relationship.

Requests for information from the authorities. Where the authorities request information regarding any of the transactions processed, the correspondent institution must always be in a position to respond promptly and must have procedures in place for obtaining the necessary information from its client institutions.

Communication between institutions. Correspondent banking relationships are, by their very nature, based on mutual trust between the participating institutions, particularly on the fact that Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) controls are being effectively implemented by the client institution. Consequently, it is important for the correspondent institution to maintain an ongoing and open dialogue with the client institution. This dialogue includes providing the necessary assistance to understand the correspondent's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) policy and its expectations regarding the controls applied by client institutions. Furthermore, where it deems appropriate, the correspondent bank shall engage with the client institution to improve its preventive controls and processes, in order to ensure that the correspondent bank has an adequate level of comfort when providing its services; otherwise, it shall inform the client institution that, should it fail to adopt the appropriate controls and processes, operations will be restricted or the correspondent relationship will be terminated.

Such communication is essential for effective monitoring, helping to identify new and emerging risks and to better understand existing ones, to clarify any incidents that may arise during the course of the business relationship, to strengthen risk mitigation measures, and to resolve any issues relating to the exchange of information.

Furthermore, within the framework of this collaboration, should the correspondent institution engage the services of a third party to provide the service to the client institution, it must provide, upon request and as soon as possible, all information obtained in the course of carrying out due diligence measures. In all cases, ultimate responsibility for Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) shall lie with the correspondent institution.

IV.4 Documentation of compliance with the obligation to apply enhanced due diligence measures.

With regard to correspondent banking, and in order to ensure compliance with the application of enhanced due diligence measures, the following must be approved internally and duly documented:

- the risk assessments carried out and the policies established;
- the procedures for decision-making regarding the establishment, maintenance or termination of correspondent banking relationships;
- the procedures for applying due diligence measures and monitoring activity;
- the internal or external control mechanisms ensuring that the procedures are correctly applied.

V. Some considerations regarding the provision of banking services to payment institutions.

Regulated entities. Payment institutions are regulated entities in accordance with the provisions of Article 2.1(h) of Law 10/2010 of 28 April, and are subject to supervision by the Commission's Executive Service to ensure compliance with regulations on Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT), and to prudential supervision by the Banco de España.

Purpose and nature of the business relationship. Where the customer is a payment institution, the financial institution must ascertain whether the money or value transfer service provider intends to use the account for its own corporate or settlement purposes, or whether it intends to use it to provide correspondent services to its own customers (i.e. that the money or value transfer system will act as a correspondent institution for its own customers).

Where a payment institution provides correspondent services to its own customers via its account, the correspondent institution must apply the measures set out in this document in order to identify risks, verify information and put in place appropriate risk mitigation measures.

Mitigation measures. To facilitate its own risk management, the correspondent institution might consider encouraging client payment institutions to open one account for carrying out their own corporate or settlement activities, and a separate account for providing correspondent banking services on behalf of their clients. This approach can facilitate effective monitoring of these two activities in line with the different types of risk they present. Separate accounts may also be considered for higher-risk activities or higher-risk customers to ensure an adequate level of transparency and effective monitoring.

APPENDIX 1
Illustrative Catalogue of High-Risk Transactions in Correspondent Banking Relationships

1) *'Bank' accounts held with other 'banks'* in which, far from involving inter-bank transactions, there are deposits and/or withdrawals of cash which, by their nature, frequency or amount, clearly appear to relate to end customers of the 'client institution', even where such transactions are not physically carried out by those customers.

2) *Correspondent accounts* used to receive or send funds to or from abroad, where there are other, more reasonable alternatives or 'routes' for such remittances.

3) *Correspondent accounts* through which transfers to or from abroad are channelled, where there is clear evidence of the total amount being deliberately split up so as not to exceed the thresholds set by the regulations on the reporting of foreign exchange transactions, and which would otherwise have been required to be reported to the authorities (such as, for example, the transactions covered by Banco de España Circular 1/2012).

4) *Correspondent* accounts in which recurring and widespread patterns are observed, suggesting that the end customers behind the 'client institution' may be operating under the same scheme or risk profile. Some indicators pointing to this scenario include:

    - A concentration of payers and/or beneficiaries; and concentrations in terms of the type of payers/beneficiaries (same country, nationality, economic sector, etc.).

    - Transfers of round sums that are clearly split into smaller amounts;

    - Similarity or identity of concepts and other patterns in transfers that suggest orchestrated manoeuvres, when, in principle, such transactions are independent of one another and have nothing to do with one another, etc.

5) *Correspondent accounts*, and in general *'bank' accounts 'held with banks',* which are being used to carry out domestic transactions on behalf of end customers. These are accounts in which transactions are carried out that, in

reality, Their aim is to conceal or put in place a 'firewall' to prevent the identification of the beneficial owners of such transactions. Some clues to detecting this intention may include, for example:

- *'Bank' accounts held with 'banks'* through which regular bill payments for individuals or companies are debited.

- *'Bank' accounts held with 'banks'* into which payments are received on behalf of individuals or companies, beyond what might be considered a mere transfer of funds in the context of correspondent banking.

6) *Correspondent banking transactions* involving the receipt or remittance of funds to or from abroad in which other aspects that raise concerns are evident (such as the use of unusual or suspicious descriptions, suspicious and conspicuously 'round' amounts in transactions where, by their very nature, this cannot be considered normal, etc.).

ANNEX 2

Risk factors in correspondent banking relationships set out in the Guidelines on risk factors issued by the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority on 26 June 2017.

Risk factors associated with the type of products, services or transactions:

Factors that may contribute to **increased risk**:

- The account may be used by other client institutions that have a direct relationship with the client institution, but not with the correspondent bank ('nesting' or correspondent clearing), which means that the correspondent bank is indirectly providing services to other credit institutions other than the client institution.
- The account may be used by other entities within the client's group that have not been subject to due diligence measures by the correspondent bank.

Factors that may help to **reduce the risk**:

- The relationship is limited to a SWIFT RMA service, designed to manage communications between financial institutions. In a SWIFT RMA relationship, the client institution, or counterparty, does not hold a payment account.
- Credit institutions are acting on their own account, rather than processing transactions on behalf of their end customers; for example, in the case of foreign exchange services between two credit institutions where both are acting on their own account and the settlement of a transaction does not involve a payment to a third party. In such cases, the transaction is on behalf of the client institution.
- The transaction relates to the sale, purchase or pledging of securities on regulated markets, for example, when acting as a custodian or using a custodian with direct access – usually via a local participant – to a securities settlement system within or outside the EU.

Risk factors associated with clients

The following factors may contribute to **an increase in risk**:

- The client institution's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) policies, and the systems and controls put in place to implement them, do not comply with the standards required by Directive (EU) 2015/849.
- The client institution is not subject to adequate supervision in the area of Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT).
- The client organisation, its parent company or an entity belonging to the same group as that organisation has recently been subject to administrative measures due to inadequate Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) policies and procedures and/or a failure to comply with AML/CFT obligations.
- The client organisation carries out significant business activities in sectors associated with higher levels of risk of Money Laundering and Terrorist Financing; for example, that organisation provides substantial money transfer services or carries out activities on behalf of certain money transfer services or currency exchange establishments with non-residents or in a currency other than that of the country in which it is established.
- The management or ownership structure of the client entity includes a person holding public office, in particular if that person is able to exert significant influence over the entity, or where their reputation, integrity or suitability as a member of the board of directors or holder of a key function gives cause for concern, or where the person holding public office comes from jurisdictions associated with a higher risk of Money Laundering and Terrorist Financing. Correspondent banks shall pay particular attention to those jurisdictions where corruption is perceived to be systemic or widespread.
- The history of the business relationship with the client institution is a cause for concern, for example, because the number of transactions is not consistent with what the correspondent would expect, given its knowledge of the client institution based on its nature and size.

The following factors may help to **mitigate the risk**: The

correspondent bank is satisfied that:

- The client organisation's controls relating to Money Laundering and Terrorist Financing are no less rigorous than those required by Directive (EU) 2015/849;
- The client institution is part of the same group as the correspondent bank, is not established in a jurisdiction associated with a higher risk of Money Laundering and Terrorist Financing, and effectively complies with the group's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) rules, which are no less stringent than those required by Directive (EU) 2015/849.

Risk factors associated with countries or geographical factors

The following factors may contribute to **an increased risk**:

- The client organisation is established in a jurisdiction associated with a higher risk of Money Laundering and terrorist financing. That is to say:
    - with significant levels of corruption or other offences underlying Money Laundering;
    - with a legal and judicial system lacking the adequate capacity to prosecute such offences effectively; or
    - without effective supervision in the area of AML/CFT.
- The client organisation carries out significant business activities with customers based in a jurisdiction associated with a higher risk of Money Laundering and terrorist financing.
- The client institution's parent company is headquartered or incorporated in a jurisdiction associated with a higher risk of Money Laundering/Terrorism Financing.

The following factors may help to **mitigate the risk**:

- The client institution is established in an EEA (European Economic Area) member state.
- The client institution is established in a third country subject to AML/CFT requirements that are no less stringent than those laid down in Directive (EU) 2015/849 and effectively applies those requirements (although correspondent banks should bear in mind that this does not exempt them from applying the enhanced due diligence (EDD) measures set out in Article 19 of Directive (EU) 2015/849).