Republic of Panama
Superintendency of Banks

RULE No. 10-2015[1]

(dated 27 July 2015)

"To Prevent the Misuse of Banking and Trust Services"

THE BOARD OF DIRECTORS
in use of its legal powers and,

WHEREAS:

Due to the issuance of Decree Law 2 dated 22 February 2008, the Executive Branch reedited Decree Law 9 dated 26 February 1998 and all its amendments as a consolidated text, and that this text was approved by means of Executive Decree 52 dated 30 April 2008, hereinafter referred to as the Banking Law;

Article 36 of Law 1 dated 5 January 1984 establishes that the Superintendency of Banks will supervise and oversee the proper functioning of the trust business;

Pursuant to paragraph 1 of Article 5 of the Banking Law, safeguarding the soundness and efficiency of the banking system is an objective of the Superintendency of Banks;

Pursuant to paragraph 2 of Article 5 of the Banking Law, strengthening and fostering favorable conditions for the development of the Republic of Panama as an International Financial Center is an objective of the Superintendency of Banks;

Article 112 of the Banking Law requires banks and other entities supervised by the Superintendency to establish policies and procedures and the internal control structures to prevent their services being used improperly for criminal purposes in Money Laundering, the Financing of Terrorism and other crimes that are related or similar in nature or origin;

Article 113 of the Banking Law sets forth that banks and other entities supervised by the Superintendency will submit the information required by law, decrees and other regulations in force in the Republic of Panama for the prevention of money laundering, the financing of terrorism and other crimes that are related or similar in nature or origin. Furthermore, they are obligated to submit this information to the Superintendency whenever it may so require;

According to Article 114 of the Banking Law banks and other entities supervised by the Superintendency will adopt policies, practices and procedures that will allow them to know and identify their clients and their employees with the greatest certainty possible. The Superintendency is authorized to develop the relevant standards in conformity with policies and regulations in force in the country;

Rule 12-2005 dated 14 December 2005 establishes the measures to prevent the misuse of banking and trust services;

By means of Law 41 dated 2 October 2000, as amended by Law 1 dated 5 January 2004, a chapter entitled "Money Laundering," was added to Title XII of the Criminal Code criminalizing money laundering;

Law 50 dated 2 July 2003 criminalized terrorism and the financing of terrorism in the Penal Code as separate crimes and established the relevant sanctions;

Law 23 dated 27 April 2015 adopted measures to prevent money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction;

Article 19 of Law 23 of 2015 designates the Superintendency of Banks, among others, as a Regulatory Body;

[1] Amended by Rule 1-2017 dated 14 February 2017, Rule 13-2018 dated 27 November 2018 and Rule 2-2019 dated 11 April 2019. Please see Resolutions SBP-GJD-0001-2014 and SBP-GJD-0003-2015.

Among the duties of the supervisory bodies, paragraph 7 of Article 20 of Law 23 of 2015 establishes issuing regulatory enforcement guidance to and feedback from regulated financial entities, regulated nonfinancial entities and for the activities of those professionals subject to supervision, as well as the procedures for identifying final beneficiaries, legal entities and other legal structures;

Pursuant to Article 22 of Law 23 of 2015 and in order to prevent money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction, the Superintendency of Banks must supervise the following entities: banks; trust companies and any other activity they conduct; finance companies; financial leasing companies; factoring companies; issuers or processors of debit, credit and prepaid cards, whether individuals or legal entities; and issuers of payment instruments and electronic money;

In accordance with Law 23 of 2015 on the prevention of money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction, the Superintendency of Banks is authorized to supervise and regulate other regulated entities besides banks and trust companies (which are already under its supervision) on the issue of the prevention of money laundering; and

During its working sessions, the Board of Directors determined it necessary and advisable to update the measures to prevent the misuse of banking and trust services established in Rule 12-2005 in order to include the new guidelines established in Law 23 of 2005 whereby measures to prevent money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction were adopted.

RESOLVES:

ARTICLE 1. SCOPE OF APPLICATION. The provisions herein are applicable the following regulated entities:

1. Banks.

2. Trust companies.

3. Banking groups pursuant to the provisions of Article 38.

ARTICLE 2. PREVENTION OF MONEY LAUNDERING, THE FINANCING OF TERRORISM AND FINANCING THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION. Banks and trust companies must take the necessary measures to prevent their operations and/or transactions being conducted with funds or proceeds from activities related to money laundering, the financing of terrorism or financing the proliferation of weapons of mass destruction, hereinafter referred to as “Prevention of Money Laundering.” For this, they are required to comply with the terms of this Rule and with the legal provisions related to this matter.

ARTICLE 3[2]. MANUAL FOR THE PREVENTION OF MONEY LAUNDERING. Banks and trust companies must have a Manual for the Prevention of Money Laundering duly approved by the Board of Directors. This manual must contain the policies, mechanisms and procedures established by the bank or trust company to prevent their operations being conducted with proceeds of these activities. The policies adopted in the Manual must permit the efficient and timely functioning of the bank’s or trust company’s system for the prevention of money laundering and must translate into rules of conduct and procedures of mandatory compliance for the entity and its shareholders.

The Manual must be disseminated to all of the bank’s or trust company’s staff and must be continuously updated.

The updates made to the Manual must be presented to the Prevention of Money Laundering Committee, which will provide preliminary approval. The changes must be ratified and approved by the Board of Directors at least once a year.

The Manual must be submitted to the Superintendency of Banks with the appropriate updates. In the event there are no updates, the bank or trust company will submit a certification signed by the

[2] Amended by Article 1 of Rule 1-2017 dated 14 February 2017.

Chairman or Secretary of the Board of Directors or by the Chairman of the Prevention of Money Laundering Committee indicating the Manual for the Prevention of Money Laundering has not been updated in the last twelve (12) months. The approval of the certification must be recorded in the Committee's minutes.

ARTICLE 4[3]. COMPOSITION OF THE PREVENTION OF MONEY LAUNDERING COMMITTEE IN BANKS. Banks must create a Prevention of Money Laundering Committee which will report directly to the Bank's Board of Directors and must be composed of at least two (2) members of the board of directors, the general manager, and the senior executives of Risk, Compliance, Business, Operations and Internal Auditing. This Committee will have among its duties the approval of the plan and coordination of the activities related to the prevention of money laundering; they must also be aware of the work conducted and operations analyzed by the Compliance Officer, such as the implementation, progress and control of the compliance program.

The Committee must draft its internal regulations, duly approved by the Board of Directors, which must contain the policies and procedures to comply with its duties, as well as the frequency with which the Committee will meet, which must be at least every two (2) months. The decisions adopted by the Committee must be recorded in minutes, which must be at the disposal of the Superintendency of Banks.

PROVISO: For branch offices of foreign banks subject to the Superintendency's host supervision that cannot meet the provisions herein because their organizational structure does not have the physical presence of the members of their board of directors in the country, the Committee will be composed of, as a minimum, the general manager and the senior executives of Risk, Compliance, Business, Operations and Internal Auditing.

ARTICLE 5. DEFINITION OF CUSTOMER. For the purposes of this Rule, "customer" will be understood as any individual or legal entity that usually or temporarily establishes, maintains or had maintained a contractual or business relationship with a Bank or that receives trust services provided by a trust company.

ARTICLE 6. FINAL BENEFICIARY. For the purposes of this Rule, "final beneficiary(ies)" will be understood as the individual(s) holding, controlling or executing a meaningful influence on the account, contractual or business relationship, or the individual in whose name or for whose benefit a transaction is conducted, including individuals ultimately controlling a legal entity, trust funds and other legal structures.

ARTICLE 7. INTERBANK OPERATIONS. Any operation or transaction resulting from an interbank relation the bank provides to foreign banks will be subject to due diligence measures commensurate with the risk they represent.

Banks are prohibited from establishing or maintaining any type of interbank or correspondent relationship with banks that do not, or whose parent company does not, have a physical presence in their home jurisdiction or are not a member of a financial group subject to consolidated supervision.

Banks must ensure they pay special attention to banks located in jurisdictions with weak standards for the prevention of money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction, in accordance with the lists issued by international organizations such as the Financial Action Task Force (FATF), among others.

ARTICLE 8. DUE DILIGENCE FOR INTERBANK OPERATIONS. For the purpose of Article 7 herein, due diligence must include, among others, the following:

1. To ensure the existence and physical presence of the bank or of its parent company and to gather enough information about:

    a. The bank receiving the contracted service.
    b. Top management
    c. Its main business activities
    d. The nature of the bank's business
    e. To determine, in conjunction with available public information, the institution's reputation.

[3] Amended by Article 2 of Rule 1-2017 dated 14 February 2017.

2. To confirm the bank receiving the service has the measures and controls to prevent and to detect money laundering, in accordance with international standards.

3. To pay special attention in the case of business with banks located in jurisdictions with Know Your Customer standards that are lower than those established by the Superintendency.

4. To clearly establish and document, if necessary, the responsibilities of each bank on the due diligence processes regarding the underlying customers in correspondent relationships.

5. To obtain top management's approval before establishing new correspondent relations.

ARTICLE 9[4]. CUSTOMER DUE DILIGENCE. In their operations, regulated entities must maintain risk-based due diligence on their individual customers and their resources subject to the contractual relationship, whether customary or temporary, regardless the amount of the transaction, and to maintain that due diligence current during the course of the transaction.

Furthermore, taking into consideration the customer's category and risk profile, banks must pay special attention when conducting transactions greater than ten thousand Balboas (B/.10,000.00), when unusual operations are detected, when money laundering is suspected, as well as when the bank has doubts on the truthfulness or integrity of the information obtained about the customer's and/or final beneficiary's identification.

Regulated entities must identify and verify the customer and/or final beneficiary, requesting and reviewing documents, data and reliable information from independent sources, such as systems or tools consolidating local or international documentation related to the prevention of money laundering (e.g. the OFAC list, United Nations list, among others).

The mechanisms for customer and/or final beneficiary identification, as well as their verification and documentation, will depend on the regulated entity's risk profile, taking into consideration the types of customers, products and services offered, distribution channels or marketing used and the geographic location of the bank's facilities, their customers and their final beneficiaries. In that regard, the following types of due diligence can be conducted:

1. **Due diligence:** The set of standards, policies, processes and actions that allow for reasonable knowledge of the customer's or final beneficiary's qualitative and quantitative characteristics, especially with regard to the customer's financial and transactional profile, the source of his/her equity and the continuous monitoring to his/her transactions and operations.

2. **Enhanced or reinforced due diligence.** A reasonably designed set of higher standards, policies, processes and actions to enhance the knowledge of the customer based on the identification, assessment and diagnosis of the risks he/she poses to the entity. This process must allow for greater knowledge of the customer's or final beneficiary's qualitative and quantitative characteristics, especially with regard to his/her financial and transactional profile, and of the source of his/her equity, and provide a more thorough, continuous monitoring to his/her transactions and operations to enhance knowledge of the customer based on the identification, evaluation and diagnosis of the risks he/she poses to the entity.

3. **Simplified due diligence:** The set of basic or essential standards, policies, processes and actions that the bank will apply to prevent money laundering crimes based on the identification, evaluation and diagnosis of risks. Among the simplified due diligence measures, banks and trust companies may reduce the process for review of documents, reduce the frequency of updates to the customer's identification, reduce monitoring related to the business or refrain from gathering information on the customer's professional or entrepreneurial activity.

The possible existing variables may increase or decrease the potential risk they represent, thus affecting the level of due diligence. Where there is greater risk, banks must take stricter measures and for lower risk, banks may adopt simplified due diligence measures, as long as there is appropriate risk analysis.

[4] Amended by Article 3 of Rule 1-2017 dated 14 February 2017.

PROVISO 1. Depending on the risk profile of each regulated entity, the Superintendency may establish different amounts for which banks must pay special attention when conducting due diligence.

PROVISO 2. Banks and trust companies must maintain their databases up to date and at the disposal of the Superintendency of Banks' supervisors.

ARTICLE 10[5]. MINIMUM DUE DILIGENCE REQUIREMENTS. Due diligence on customers and their resources, whether individuals or legal entities, consists of at least the following actions:

1. Prepare a customer profile.

2. Maintain the documentation and follow-up on their customers' financial transactions.

3. Give special follow-up to those customers conducting operations equal to or greater than ten thousand balboas (B/.10,000.00), taking into account the customer's category and risk profile.

4. Establish a procedure containing the approval levels and customary amounts for any customer to conduct cash operations equal to or greater than ten thousand balboas (B/.10,000.00).

5. Review, at least every six (6) months, their customers' operations, both habitual and in cash of amounts equal to or greater than ten thousand balboas (B/.10,000.00), in order to determine if they follow the criteria for habitual operations established by the bank.

6. Pay special attention to and take pertinent measures for those high profile customers, including those identified as Politically Exposed Persons (PEP).

Banks and trust companies members of a banking group may consolidate their processes of due diligence within the compliance structure of the banking group. In these cases, the regulated entity will always remain accountable.

ARTICLE 11[6]. METHOD FOR CUSTOMER RISK CLASSIFICATION. Every regulated entity must design and adopt a method for customer risk classification that must contain, as a minimum, the following elements:

1. General concept.

2. Minimum criteria or variables for analyzing the customer's risk profile.

3. Description of customer risk classification and categories.

4. Definition of models for establishing the customer's risk profile.

5. Design and description of risk matrixes.

6. Definition of a procedure for updating the customer risk classification containing the authorization process for changing a customer's risk classification. If the customer risk assessment is determined by an automated monitoring tool, the established procedure must ensure that all data on the changes made to the customer's risk profile are retained in the system.

The methodology for customer risk classification and its updates must be approved by the Prevention of Money Laundering Committee and submitted to the Superintendency of Banks annually to be verified. In the event there are no updates, the bank or trust company must submit a certification signed by the Chairman or Secretary of the Board of Directors or by the Chairman of the Prevention of Money Laundering Committee indicating the methodology has not been updated in the last twelve (12) months. The approval of the certification must be recorded in the Committee's minutes.

The Superintendency of Banks will verify that the methodology for customer risk classification is reasonable in accordance with the volume and nature of the operations conducted by the regulated entity, as well as the risk profile of the customer the entity is serving. In those cases

[5] Amended by Article 4 of Rule 1-2017 dated 14 February 2017.
[6] Amended by Article 5 of Rule 1-2017 dated 14 February 2017.

where it is determined that the method for classification is insufficient or inappropriate, the Superintendency may ask the regulated entity to take the relevant measures to remedy or clarify them within a period the Superintendency will establish.

ARTICLE 12. CUSTOMER RISK CATEGORIES. Regulated entities must assign a risk category to every customer based on the description of each particular risk profile, for which the regulated entity must design and implement a methodology for customer risk classification. Regulated entities must take into consideration this classification to establish the type of due diligence and the applicable monitoring programs.

To establish the customers' category risk profile, the following aspects will be considered, as a minimum:

1. Differentiation of the relationship with customers by risk category, depending on whether they are in high-, medium- or low-risk categories.

2. Criteria for establishing risk categories.

3. Additional documentation requirements to comply with the "Know your customer and/or final beneficiary" policy for each risk category established by the regulated entity.

ARTICLE 13. MINIMUM CRITERIA OR VARIABLES TO ANALYZE AND DESCRIBE A CUSTOMERS' RISK PROFILE. To analyze and describe each customer's risk profile, regulated entities will choose among the following criteria or variables, without being limited to them:

1. Citizenship.

2. Country of birth or country of incorporation.

3. Country of domicile.

4. Profession or occupation.

5. Geographic zone of the customer's business activities.

6. Customer's economic and financial activity.

7. Type of legal structure used, when applicable.

8. Type, amount and frequency of transactions (sent and received, national and international).

9. Source of resources (national and international).

10. Politically exposed persons (PEP).

11. Products, services and channels used by the customer.

The criteria or variables used to analyze and describe a customer's risk profile must be described in the methodology for customer risk classification used by the bank.

ARTICLE 14[7]. CUSTOMER PROFILE FOR INDIVIDUALS. For individuals, banks and trust companies must prepare a customer profile that will include the form designed by the entity containing written information, as well as the documents supporting that information. As a minimum, the customer profile must contain the following information and documentation, which must be obtained before entering into the business relationship with that customer:

1. **Customer identification and verification:** Full name, age, gender, employment or employment status, marital status, profession or occupation, citizenship, residency and a suitable personal identification document.

   For the purposes of the suitable personal identification document, the personal identification card, or the official personal identification card application form while this document is being processed, will be used in the case of a Panamanian citizen. The

[7] Amended by Article 6 of Rule 1-2017 dated 14 February 2017, by Article 1 of Rule 13-2018 dated 27 November 2018 and by Article 1 of Rule 2-2019 dated 11 April 2019.

passport will also be acceptable for those Panamanian citizens living abroad. The tax identification number from the country or countries where the individual has his fiscal residence will also be required in order to maintain the information related to his tax identification number up to date.

The suitable personal identification document will be the passport for foreigners. Foreigners must also provide:

a. The tax identification number of the country or countries where the individual has his fiscal residence in order to maintain the information related to his tax identification number up to date, and

b. An affidavit indicating that the inflow and outflow of money made within the financial entity meet and will meet the tax obligations of his country or countries of fiscal residence.

   According to the Banking Law, banks are authorized to cooperate with any investigation conducted by law enforcement agencies.

To meet the passport requirement, it will only be necessary to keep a copy of the page(s) where the customer's picture, signature and general information appear, as well as the page bearing the "entering the country" stamp. The requirement for a copy of the pages of the passport bearing the entering the country stamp is not applicable if the customer was accepted by the bank or trust company through visits abroad or when acceptance was made by companies affiliated to the group or by international license banks. These customers may also be identified by the official identification card from their home country bearing their picture, general data and signature.

Foreigners that have obtained residency in Panama may also be identified through the personal identification card issued by the Electoral Court of Panama.

People in our country under a permanent residency migratory status as a refugee or asylee may be identified through the refugee identification card issued by the National Immigration Service.

In all cases, the document must be current when submitting it for opening accounts.

For the purposes of updating the relevant files, the bank may update expired identification cards by verifying the database of the Electoral Court without requiring the customer to physically submit the document. Expired passports must be updated by the customer.

PROVISO: The affidavit referred to in (b) herein may be satisfied by a single, independent document or as part of the customer profile form.

2. **Origin and destination of resources or equity:** It is understood that the origin and destination of resources refers to: as origin, the jurisdiction(s) from which most of the funds are coming, or as destination, where the funds are sent to. This will always refer to geographical issues.

3. **Customer financial profile and source of resources or equity:** It is understood that the source of resources refers to the written proof of the origin of funds used to conduct any transaction.

   The financial profile will be understood as the result of the joint analysis of the demographic and socioeconomic characteristics and variables submitted by a customer and verified by the entity when entering into a relationship, which must be augmented by updated and historical information. For such purposes, the customer must submit at least one of the following documents: job letter, social security tab, tax return, pay stub or any other legal or contractual documentation verifying the customer's income.

   Furthermore, all reasonable measures for supporting the origin of funds, frequency of movements, geographic origin and whether the customer pays in cash, quasi-cash, checks or wire transfers will be taken into account at the beginning and during the contractual relationship to establish the usual behavior the customer will maintain with the reporting entity.

4. **Customer transactional profile:** It will be understood as the comparison between the expected financial profile and the frequency and capacity of a customer's real transactions in one or various timeframes.

   The customer's financial information must be examined and the analysis of the quantity and volume of the transactions must be documented in the physical or digital file to establish the expected monthly or annual customer transactional profile when entering into the relationship.

   During the contractual relationship, the bank or trust company must monitor and verify that the financial operations made by the customer do not show material inconsistencies regarding the expected transactional profile that was determined when entering into the relationship.

   When assigning a risk level to the customer, the bank or trust company must consider as criteria within the risk classification method, whether the origin and/or destination of the resources come from or are sent to jurisdictions considered to have weak measures against tax evasion or come from or are sent to jurisdictions that are non-cooperative in this matter.

5. **Other additional aspects to consider:**

   a. In cases when the customer is acting as the intermediary for the final beneficiary or owner of the operation, banks and trust companies must conduct due diligence on that final beneficiary.

   b. Banks and trust companies must understand and, as applicable, obtain information on the planned purpose and character of the business or professional relationship.

   c. Any new account or contract must comply with the assessment of the customer's financial and transactional profiles, in order to measure the risk of products or services offered.

   d. Banks and trust companies must have documentation in the relevant file of all actions taken to properly identify their customer and/or final beneficiary.

   e. Any service resulting from a relationship between a bank or trust company and a foreign customer will be subject to due diligence measures in conformance with the risk level the customer represents based on the international parameters and standards and internal policies and control procedures established by the entity.

All information required herein must be consolidated in one file, whether physical or digital.

ARTICLE 15[8]. CUSTOMER PROFILE FOR LEGAL ENTITIES. For legal entities, banks and trust companies must prepare a customer profile that will include the form designed by the entity containing written information, as well as the documents supporting that information. As a minimum, the customer profile must contain the following information and documentation:

1. **Customer identification and verification:** Legal entity's full name, registration data, domicile, address and phone numbers. For Panamanian legal entities, the tax identification number (RUC) will be required when applicable. For foreign legal entities, the tax identification number of the country or countries where they have their fiscal residence, when applicable. The bank or trust company must also request an affidavit indicating that the inflow and outflow made within the financial entity meet and will meet the tax obligations of the country or countries where they have their fiscal residence.

   Trust companies must fully know and understand the information on the purpose of the trust fund.

   PROVISO: The affidavit referred to herein may be satisfied by a single, independent document or as part of the customer profile form.

[8] Amended by Article 7 of Rule 1-2017 dated 14 February 2017, Article 2 of Rule 13-2018 dated 27 November 2018 and Article 2 of Rule 2-2019 dated 11 April 2019.

2. **Certifications verifying the incorporation and existence of the legal entity:** The requisite to obtain certifications verifying the incorporation and existence of the legal entity will be met as follows:

   a. Copy of the Articles of Incorporation for a Panamanian legal entity or its equivalent for a foreign legal entity.

   b. For a Panamanian legal entity, the original or copy of the Public Registry certification or information extracted by the customer or the legal entity from the Public Registry's database verifying the existence of and information on the legal entity.

   c. For a foreign legal entity, the documents equivalent to that of the provisions of paragraph 2 verifying the incorporation and existence of the foreign legal entity.

3. **Identification of dignitaries, directors, agents and legal representatives:** Banks and trust companies must identify dignitaries, directors, agents and legal representatives of the legal entities. For such purposes, banks and trust companies will only require a copy of the personal identification card of the chairman and/or legal representative, as the case may be, the secretary and the people appointed as signatories and agents of the legal entity. Trust companies must identify the custodian, advisor or people making decisions on the trust fund's equity and its distribution, whichever is the case.

4. **Identification of the final beneficiary:** Banks and trust companies must take reasonable measures to identify the final beneficiary using relevant information obtained through reliable sources. For such purposes, banks and trust companies must understand the nature of the customer's business and its shareholding and control structure. If a legal entity is the final beneficiary, the due diligence will be expanded until the individual who is the owner or controller is identified.

   To identify the final beneficiary of corporations, reporting entities must make the relevant efforts to identify shareholders holding a percentage equal to or greater than ten percent (10%) of the issued shares of the relevant corporation, with the reporting entities requiring a copy of the personal identification document of each of these shareholders. Listed companies are exempt from identifying their final beneficiary, with the exception of those incorporated in countries classified as non-cooperative by the Financial Action Task Force (FATF). The data on the nationality, country of birth and country of residence must be obtained for all of [the individuals above].

   The bank or trust company must maintain the support documentation certifying that the company is listed on the stock exchange in the file.

   For foreigners belonging to jurisdictions with which Panama has entered into international agreements for the exchange of tax information duly ratified by the Republic of Panama and fully in force, the bank and trust company must ensure it has the information on the country and the [subject's] tax identification number for the country or countries of fiscal residence, in order to maintain the information related to the tax identification up to date.

   For public entities (state-owned corporations) whose final beneficiary is the Panamanian State or a Foreign State, banks and trust companies must identify and take reasonable measures to verify the identity of the individual holding the highest administrative position.

   For other legal entities whose final beneficiaries cannot be identified by shareholding, the reporting entity must ensure it obtains a certificate, certification or affidavit duly signed by the representatives or authorized persons, in which the final beneficiary(ies) is (are) listed.

   When the reporting entity is not able to identify the final beneficiary, it will refrain from entering into or continuing the business relationship or conducting any transaction as long as there is any persistent doubt as to the identity of the customer or final beneficiary.

5. **Treatment of legal entities with offshore operations.** For Panamanian or foreign legal entities conducting offshore operations and having accounts in a bank in Panama, the bank must request an affidavit certifying that the resources deposited in those accounts have complied and will comply with the relevant tax obligations.

6. **Origin and destination of resources or equity:** It is understood that the origin and destination of resources refers to: as origin, the jurisdiction(s) from which most of the funds are coming, or as destination, where the funds are sent to. This will always refer to geographical issues.

7. **Customer financial profile and source of resources or equity:** It is understood that the source of resources refers to the written proof of the origin of funds used to conduct any transaction.

   The financial profile will be understood as the result of the joint analysis of the demographic and socioeconomic characteristics and variables submitted by a customer and verified by the entity when entering into a relationship, which must be augmented by updated and historical information. For such purposes, the legal entity must submit at least one of the following documents: financial statements, duly signed, a tax return or any other legal or contractual documentation verifying the customer's income.

   Furthermore, all reasonable measures for supporting the source of funds and the geographic origin of the funds, frequency of movements and whether the customer pays in cash, quasi-cash, checks or wire transfers will be taken into account at the beginning and during the contractual relationship to establish the usual behavior the customer will maintain with the reporting entity.

8. **Customer transactional profile:** It will be understood as the comparison between the expected financial profile and the frequency and capacity of a customer's real transactions in one or various timeframes.

   When assigning a risk level to the customer, the bank or trust company must consider as criteria within the risk classification method, whether the origin and/or destination of the resources come from or are sent to jurisdictions considered to have weak measures against tax evasion or come from or are sent to jurisdictions that are non-cooperative in this matter.

ARTICLE 16[9]. IDENTIFICATION OF THE FINAL BENEFICIARY IN CORPORATIONS. For the purposes of the provisions of paragraph 5 of Article 15 regarding the identification of shareholders holding a percentage equal to or greater than ten percent (10%) of the issued shares of the corporation, banks and trust companies must request documents verifying the name of the individual identified as the final beneficiary and holder of the shares of the corporation, regardless of whether they are nominative or bearer shares.

1. In case of nominative share corporations, banks and trust companies must require at least one of the following documents:

   a. Copy of the share certificate verifying the name of the owner of nominative shares that have been issued.

   b. Affidavit signed by the Chairman or Secretary providing the information on the owners of nominative shares and the percentage held by each.

   c. Copy of the share registry.

2. For corporations issuing bearer share certificates after the enactment of Law 47 of 2013 adopting a custody regime applicable to bearer shares, regulated entities must request the following from the customer that maintains this type of shares:

   a. Copy of the minutes of the board of directors or shareholders meeting registered in the Public Registry, authorizing the corporation to accept the custody regime created by Law 47 of 2013.

   b. Certification of the authorized custodian certifying who owns the bearer shares issued by the corporation, in order to determine the final beneficiary –i.e. the relevant individual.

3. For foreign bearer share corporations, they will be required to comply with the provisions of paragraph 2 in determining the final beneficiary – i.e. the relevant individual.

[9] Amended by Article 8 of Rule 1-2017 dated 14 February 2017.

ARTICLE 17[10]. SIMPLIFIED DUE DILIGENCE. Without prejudice to the risk assessment conducted by the reporting entity, the bank or trust company may conduct a simplified due diligence for the cases the Superintendency of Banks establishes, making sure they have gathered the following information:

1. **Customer identification and verification:** Full name, age, gender, employment or employment status, marital status, profession or occupation, citizenship, residency and a suitable personal identification document. The bank or trust company must verify the name and identification card number with the information held by the Civil Registry, as well as [verifying all] other data furnished by the customer.

2. Any other document that the bank deems necessary to document according to the type of customer and his/her activity.

Simplified due diligence will be applicable only in the following cases:

1. Simplified process accounts, according to the parameters established in Rule 1-2013, because of their low transaction movements with an established quantitative threshold;

2. Christmas savings accounts;

3. Accounts opened exclusively for payroll payment, as long as the accountholder or employer document the income earned by the employee holding the account, which will be understood as the information referred to in the customer profile for individuals;

4. School or educational savings accounts, if they are payable on an established schedule; or those savings accounts without a specific withdrawal or cancellation period opened by minors or their legal representatives within banks authorized by Law for such purposes;

5. The savings accounts meant to pay subsidies or social welfare programs by the Government of the Republic;

6. Checking or savings accounts whose holders are individuals whose balance does not exceed five thousand balboas (B/.5,000.00) at any time. In these cases, the financial profile will be supported with a customer's affidavit on his/her income (see Appendix I) and the bank or trust company must have the parametric tools to permit continuous monitoring of the balance to prevent the established limit being exceeded. In the event the customer exceeds the five thousand balboas (B/.5,000.00) balance, the bank must make sure it has requested all the data required by Article 14 of this Rule;

7. Checking or savings accounts opened exclusively to be used through e-wallets for business-to-business or business-to-person operations. In these cases, the customer financial profile may be verified through documentation showing the business relationship and the volume of operations with suppliers or distributors;

8. The accounts opened for withholding property taxes;

9. Any other product that, with the bank's prior risk assessment, is aimed at financial inclusion and represents a low risk level, as long as that product has been previously approved by the Superintendency for such purposes.

ARTICLE 18. DUE DILIGENCE FOR WIRE TRANSFERS. Banks must make sure of appropriately applying due diligence procedures when conducting wire transfers, for which the bank must gather the following information:

1. Name of the originator.

2. Name of the beneficiary.

3. Account number for each one or a single reference number for the transaction.

4. Amount transferred.

[10] Amended by Article 9 of Rule 1-2017 dated 14 February 2017 and Article 3 of Rule 13-2018 dated 27 November 2018.

The bank must have efficient security procedures and measures to prevent customer misuse of wire transfers, for which the bank must ensure it has a system which provides the relevant warnings in cases where these transfers are unusual in accordance with Rule 7-2015 covering the warning signs related to wire transfers.

ARTICLE 19[11]. BANK AND TRUST COMPANY RISK ASSESSMENT. Money laundering risk management must be an integral part of the bank's and trust company's risk assessment. This assessment process must be conducted by the Risk Unit along with the Prevention of Money Laundering Unit and must be approved by the board of directors of the entity.

The risk assessment process must be reviewed at least once every twelve (12) months and the results obtained must be presented to the board of directors. The management must define corrective action plans to remedy proven weaknesses, describing the actions, responsible persons and timeframe for their remedy. The minutes of the board of directors must include the mechanisms approved for the verification of their compliance. This risk assessment must be submitted to the Superintendency of Banks annually.

ARTICLE 20. DOCUMENTATION AND FOLLOW UP. Banks and trust companies must maintain all of their customer and/or final beneficiary documentation and follow up on the transactions conducted by them during the course of the contractual relationship to identify unusual operations. Regulated entities must have tools to detect abnormal or suspicious activity patterns in all the transactions maintained with their customers. For such purposes, banks and trust companies must take the following measures:

1. To follow up on the operations conducted throughout the business relationship to verify that they match the customer's professional or entrepreneurial activity, financial and transactional profile. Banks and trust companies will increase their follow up when noticing warning signs or behavior above average risk in accordance with the regulations or because it resulted from the risk analysis conducted by the regulated financial entity.

2. To periodically review documents, data and information obtained as a result of the application of due diligence measures, to ensure they are updated and conform to the true operations of the customer.

3. To periodically read documents, data and reliable information from independent sources, such as tools or systems consolidating domestic and international information related to money laundering prevention.

4. To pay special attention to the financial and transactional profile to cash, quasi-cash, checks and wire transfer movements, among others.

ARTICLE 21[12]. MONITORING TOOL. Banks and trust companies must have transactional review and monitoring systems that must generate automatic and timely warnings on transactions at variance with the customer's expected behavior and other warnings permitting the identification of the different types, as well as reports including, as a minimum but not limited to, the following:

1. Customer data

2. Transaction history

3. Existing relationship between the accounts of each customer with that of other customers and other products or services within the entity.

4. Historical information on the risk category assigned to each customer.

5. Warning signs generated.

6. Statistics on the warning signs generated, processed, in progress and pending processing, with their respective supporting documentation.

The regulated entity must appoint suitable and responsible staff as the administrator of the review process.

[11] Amended by Article 10 of Rule 1-2017 dated 14 February 2017.
[12] Amended by Article 11 of Rule 1-2017 dated 14 February 2017.

The Bank or trust company must review all warning signs to identify unusual operations to which must be reviewed.

Discarded unusual transaction warning signs require evidence of the reason for the rejection and the retention of digital or hardcopy documentation to support it.

ARTICLE 21A[13]. FREEZING OF ASSETS. For the purposes of the provisions of Article 49 of Law 23 of 2015, banks and trust companies must draft policies and procedures for freezing terrorist funds, assets or property once the lists issued by United Nations Security Council are received.

ARTICLE 22. POLITICALLY EXPOSED PERSONS. Banks and trust companies must adopt enhanced or reinforced due diligence measures for customers and/or final beneficiaries that are politically exposed persons, whether citizens or foreigners, and pay special attention and take appropriate measures for these customers.

In accordance with the provisions of Paragraph 18 of Article 4 of Law 23 of 2015, politically exposed persons (PEP) are citizens or foreigners that serve high-ranking public functions with authority and jurisdiction in a State or international organism. As examples, these can include Heads of State or of Government, high-level politicians, high ranking governmental, judicial or military officials, senior executives of state companies or corporations, public officials holding elected office, among others, that are part of the decision-making in public entities; persons holding or who have been entrusted with important functions in an International Organization. It refers to those who are members of senior management, i.e. directors, deputy directors and members of the Board of Directors or its equivalent functions.

A person is considered PEP from his appointment until his removal from office and for a period of two (2) years following the cessation of the duties and obligations that caused him to be considered a PEP.

Regulated entities must establish appropriate risk management systems and conduct deeper due diligence, including the following aspects:

1. To have tools that will permit conducting relevant actions to determine whether the customer or final beneficiary is a politically exposed person.

2. To obtain top management's approval to establish (or to update the profile, in case of existing customers) business relations with these customers, if applicable.

3. To identify the PEP's financial and transactional profile regarding the source of equity and source of funding, if applicable.

4. To conduct intensified continuous follow up of the operations throughout the contractual relationship.

In the case of close relatives of politically exposed persons, i.e. spouse, parents, siblings and children, as well as people known to be close to these persons, regulated entities must apply these due diligence measures.

ARTICLE 23[14]. DUE DILIGENCE FOR HIGH-RISK CUSTOMERS. Regulated entities must adopt enhanced or reinforced due diligence measures for customers and/or final beneficiaries classified as high-risk customers and must take relevant measures for these customers.

For high-risk customers, regulated entities must establish appropriate risk management systems and conduct deeper due diligence, including the following actions:

1. Obtain top management's approval to establish (or to update the profile, in case of existing customers) business relations with these customers, if applicable.

2. Conduct intensive continuous follow up on their operations throughout the contractual relationship.

Without prejudice to customers considered high risk according to the Bank's or trust company's risk assessment, the following individuals will be considered high-risk customers:

[13] Added by Article 12 of Rule 1-2017 dated 14 February 2017.
[14] Amended by Article 13 of Rule 1-2017 dated 14 February 2017.

1. Politically exposed persons (PEP).

2. Customers using large amounts of cash.

3. Customers with equity or partners coming from territories or countries considered non-cooperative jurisdictions by the Financial Action Task Force (FATF).

4. Anyone else the regulated entity classifies as a high-risk customer.

ARTICLE 24. CASH AND QUASI-CASH TRANSACTIONS REPORT. Regulated entities must report the following transactions or operations, conducted within the Republic of Panama or abroad, as well as any other information related to these activities using the forms established by the Financial Analysis Unit:

1. Cash or quasi-cash deposits or withdrawals conducted in individual or legal entity accounts in the amount equal or greater than ten thousand balboas (B/.10,000.00). Foreign currency operations must be reported in the equivalent of the exchange.

2. Successive deposits or withdrawals of money in close proximity that, although individually under ten thousand balboas (B/.10,000.00), at the end of the day or week total an amount equal or greater than ten thousand balboas (B/.10,000.00). In these cases, the bank or trust company will report the cumulative value of the operations at the end of the business week through the mechanism provided by the Superintendency of Banks for that purpose. The reporting entity must maintain any documentation supporting the timely and accurate submittal of data within the reports mentioned herein in its files and at the disposal of the Superintendency of Banks.

3. The exchange of cash from lower denominations to higher denominations or vice versa, in an amount equal or greater than ten thousand balboas (B/.10,000.00), or through successive transactions that, although individually are under ten thousand balboas (B/.10,000.00), at the end of the day or week total an amount equal or greater than ten thousand balboas (B/.10,000.00).

4. Cashing cashier's checks, traveller's checks, payment orders, checks paid to the order of the bearer, checks with blank endorsements and issued on the same date or close dates by the same drawer or drawers of the market.

5. Purchase and sale of currency other than the legal currency in the Republic of Panama, equivalent or greater than ten thousand balboas (B/.10,000.00), or the total of that amount in a week, or through successive transactions that, although individually are under B/.10,000.00, at the end of the day or week total an amount equal or greater than ten thousand balboas (B/.10,000.00), must be reported by the equivalent of the exchange.

6. Cash or quasi-cash payments or collections for an amount equal or greater than ten thousand balboas (B/.10,000.00), or the total of that amount in a week by the same customer or a third party acting on behalf of the customer.

ARTICLE 25. REVIEWING, UPDATING AND MAINTAINING DOCUMENTS. Banks and trust companies must maintain all information and documentation obtained during the due diligence process up to date. They will also keep, by any means authorized by Law and for a period of not less than five (5) years from the date the contractual relationship with the customer was terminated, a signed set of the due diligence forms for individuals as well as the legal entities, a copy of the documents obtained through the due diligence process, the documents supporting the operation or transaction and any other document that will permit reconstructing the customers' individual operation or transaction, if necessary.

Customer and/or final beneficiary documents and data must be updated in accordance with the policy adopted by each regulated entity for those customers that have no changes in their risk profile, pursuant to the following parameters:

1. High-risk customers: review or update the customer data at least every twelve (12) months.

2. Medium- or moderate-risk customers: review or update customer data at least every twenty-four (24) months.

3. Low-risk customers: review or update customer data at least every forty-eight (48) months.

This policy must establish the immediate update of the customer and/or final beneficiary information when there are substantial changes in the transactional profile and when the customer's classification is high-risk or when there is any sudden change in the risk profile.

ARTICLE 26. KNOW YOUR CUSTOMER AND/OR FINAL BENEFICIARY POLICY MANUAL. Banks and trust companies must have a compliance policies, procedures and internal controls manual, approved by the Board of Directors and with the prior approval of the Prevention of Money Laundering Committee, to conduct the "know your customer and/or final beneficiary" policy, which must be reviewed on an annual basis and updated whenever necessary. These policies and procedures will be adjusted to the degree of complexity of the bank's or trust company's activities and may cover different customer categories based on the potential for illegal activity related to operations or transactions made by those customers.

ARTICLE 27[15]. KNOW YOUR EMPLOYEE POLICY. Banks and trust companies must appropriately recruit their employees and supervise their behavior, especially those performing customer service, money acceptance and information control duties. Furthermore, banks and trust companies must establish an employee profile that will be updated while the labor relationship lasts.

The employees must be trained on understanding the risks to which they are exposed, the controls mitigating such risks and the impact of their actions on a personal and institutional level.

In addition, employers must provide codes of conduct guiding the actions of each of their employees, managers and directors for the proper development of the system for the prevention of money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction and the establishment of measures for ensuring the requirement for the confidentiality of the information on the system for the prevention of money laundering.

The code of conduct must contain, as a minimum, the guiding principles, values and policies highlighting the mandatory character of the procedures integrating the system for the prevention of money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction in accordance with the existing regulations on the matter. Similarly, the code must establish that any infringement of the prevention system will be considered an infraction that will be punished according to the seriousness of the infringement.

ARTICLE 28. OBLIGATION TO TRAIN EMPLOYEES. Banks and trust companies must provide continuous and specific training to their employees in the business and operating areas performing duties related to dealing, communicating and handling customers and suppliers, receiving money, processing transactions, designing products and services, and the staff working in sensitive areas such as compliance, risk, human resources, technology and internal auditing. The objective of this training is to provide staff updated information on the different Money Laundering types, cases and regulations. The training to be conducted is:

1. **Orientation training for new employees:** Regulated entities must develop and implement orientation training programs on prevention of money laundering, addressed to new employees, containing the following topics, as a minimum:

    a. General concepts on the prevention of money laundering.
    b. Current prevention of money laundering legislation.
    c. Contents of the Compliance Manual.
    d. Due diligence and know your customer procedures.
    e. Warning signs.
    f. Responsibilities and criminal, administrative and internal sanctions.

2. **Annual training for the entity's staff, pursuant to the provisions of this article:** Regulated entities must develop and implement an annual training program to maintain current staff updated on the policies, procedures and internal controls to prevent the misuse of services provided, as well as the different criminal modalities used for money laundering. This training must also include the following:

    a. Procedures adopted by the entities to comply with the provisions herein.

[15] Amended by Article 14 of Rule 1-2017 dated 14 February 2017.

b. Analysis of the current legislation, including the implications for the regulated entity and its employees.
c. Responsibilities of the Auditing, Compliance and Business Departments.
d. Recommendations issued by international organizations.
e. Analysis and development of current cases related to money laundering crimes.

Training programs conducted by banks and trust companies must have mechanisms to evaluate results obtained, in order to determine the effectiveness of those programs and the extent of the proposed objectives.

Banks and trust companies must maintain a record of training provided to employees, as well as the date, venue and duration of that activity, the name of attendees, their positions and the agenda developed during the training.

Statistics with the results of this training must be provided to the Prevention of Money Laundering Committee to guarantee the relevant corrective actions were conducted.

ARTICLE 29. UNUSUAL OPERATIONS. Banks and trust companies must deepen the analysis of unusual operations to obtain additional information that will permit them to confirm or dismiss the anomaly, certifying in writing the conclusions reached and the supporting documentation verified.

When the regulated entity identifies an unusual operation, it must start a review of the events that will contain, as a minimum, the following information:

1. Customer identification.

2. Economic activity.

3. Background of the operation, e.g. historical statements of the account, check deposits, wire transfers, among others.

4. Detailed description of movements or transactions studied or analyzed.

5. Conclusions and recommendations on the analyzed case.

Regulated entities must create a log of unusual operations that were investigated by the regulated entities, regardless of whether they led to their being reported as suspicious operations.

ARTICLE 30[16]. SUSPICIOUS OPERATIONS. Banks and trust companies must directly inform the Financial Analysis Unit of any event, transaction or operation that has been conducted, including attempts to conduct those operations, which is suspected of being related to or involved with the crimes of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction, regardless of the amount and whether or not it can be confirmed or substantiated. [This requirement includes] any failure in controls.

The Compliance Officer will conduct the internal analysis of the unusual and/or suspicious operations resulting from matching the customer's profile with its monitoring systems.

When, during the course of their activities, reporting entities become aware of operations classified as suspicious operations that cannot be supported or substantiated, they must comply with the following actions:

1. Create a log containing operational information. The information will contain the data on the contractual relationship originating the operation, the date(s), the amount(s) and the type(s) of operations. This log must succinctly include the remarks of the employee detecting the operation.

2. Notify the Compliance Officer of the suspicious operation. The Compliance Officer will order a review of the operation to verify its suspicious nature and will succinctly include his respective remarks.

3. Notify the Financial Analysis Unit for the Prevention of Money Laundering and the Financing of Terrorism (UAF, for its acronym in Spanish) of the suspicious operation using the forms established for that purpose. The notification will be made through the

[16] Amended by Article 3 of Rule 2-2019 dated 11 April 2019.

Compliance Officer immediately following the detection of the suspicious event, transaction or operation. In the event that gathering all of the information previously sent is complex or requires clarifications to be precise or accurate, the reporting entities must update the information previously sent to the Financial Analysis Unit (UAF) expeditiously through a supplementary suspicious transaction report.

4. Register in the log the date and the form for notification of the Financial Analysis Unit for the Prevention of Money Laundering and the financing of terrorism (UAF), as well as the date and number of the reply issued by the Unit;

5. Update the relevant file in the case of suspicious operations.

6. If necessary, attach charts, tables, notices or any other information that will permit the visualization of the suspicious operation that was the object of the report.

ARTICLE 31. WARNING SIGNS. The Superintendency of Banks has established, by a Rule, a warning signs catalog for those signs that deserve a closer look by regulated entities in order to determine, along with other elements for analysis, whether they are suspicious operations that may be related to money laundering. The Superintendency may, from time to time, modify that catalog when it deems it appropriate, by means of a Rule.

ARTICLE 32. NOTIFICATION TO THE FINANCIAL ANALYSIS UNIT (UAF). The Superintendency of Banks will notify the Financial Analysis Unit (UAF) of any suspicious operations it is aware of in the course of bank and trust company examinations, without exempting the entity from the obligation to do so.

ARTICLE 33. FURNISHING OF INFORMATION. In accordance with the provisions of Article 113 of the Banking Law, Banks are required to furnish a copy of the suspicious transactions report submitted to the Financial Analysis Unit (UAF) when the Superintendency requests the information.

ARTICLE 34. COMMUNICATION WITH THE FINANCIAL ANALYSIS UNIT (UAF). In cases where the bank or the trust company deems it advisable to close any bank account, trust management or trust fund linked to a reported suspicious transaction, they must submit a written report to the Financial Analysis Unit (UAF), in addition to the initial suspicious transaction report, within a period of not more than ten (10) business days from the date of that closure.

The report must include information on the closure of the relevant account, the method used by the bank or trust customer to withdraw funds and the follow-up given to those when it can be determined. A copy of the closure form and the document used by the user to withdraw the funds must be attached to the report.

ARTICLE 35. PROTECTION OF EMPLOYEES, DIRECTORS AND AGENTS. Banks and trust companies shall adopt appropriate measures to maintain confidentiality on the identity of their employees, directors or agents that have made any report or communication to the internal prevention bodies of the regulated entity.

ARTICLE 36. CORPORATE LIABILITY. For the exclusive purposes of sanctions, the acts and behaviors of the directors, dignitaries, senior executives, administrative or operations staff of banks and trust companies will be attributable to those entities and to the persons exercising activities on whose behalf they act.

Individuals who are the authors of those acts and behaviors will be subject to the relevant civil and criminal liabilities.

ARTICLE 37[17]. INTERNAL AUDITING. The Bank's internal auditing unit is responsible for continuously assessing and reviewing the internal control system and compliance with Money Laundering risk management policies.

Internal auditing duties must be independently managed and the staff must be suitable and properly trained on issues of the prevention of money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction.

[17] Amended by Article 15 of Rule 1-2017 dated 14 February 2017.

ARTICLE 38[18]. BANKING GROUPS. The holding company of banking groups to which the Superintendency of Banks is the home supervisor must ensure that they comprehensively manage group-level money laundering risk, as well as assessing the potential risks associated with the activities identified by their branch offices, affiliated companies and subsidiaries when so required. Furthermore, they must have policies and procedures that will allow them to determine the customer's risk exposure in other branch offices, affiliated companies or subsidiaries belonging to the same economic group.

The Superintendency will have access to customer information that will permit it to comply with this provision regarding the banking group's institutions that conduct operations directly with the bank. The Superintendency of Banks must ensure that the banking group applies rules and procedures equivalent to those adopted by the bank, especially with regard to customer due diligence measures.

For the purposes of the provisions in this Article and according to the guidelines established by FATF, the banking groups subject to the consolidated supervision of the Superintendency must develop corporate policies and procedures for the system to prevent money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction, including:

a) Group-level policies and procedures for risk management and for the prevention of money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction;

b) Policies and procedures for the exchange of information within the group for the purposes of preventing money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction.

   These policies and procedures must include, but are not limited to, the exchange of information, the analysis of unusual operations and suspicious transactions reports. To this end, the branch offices, affiliated companies, subsidiaries and non-banking entities related to the banking group itself, must receive this type of information when it is relevant and pertinent for an appropriate risk management.

   This exchange of information within the banking group is not considered a disclosure of information to third parties and therefore does not contravene the provisions of Article 56 of Law 23 of 2015;

c) The criteria necessary to be adopted by the members of the banking group to guarantee the highest standards when hiring employees and appointing directors and managers;

d) Training programs on the prevention of money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction.

The type and scope of the aforementioned policies and procedures must take into consideration the risks of money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction and be consistent with the sophistication of operations and/or services offered, as well as the size of the banking group.

ARTICLE 38A[19]. BRANCH, AFFILIATED OFFICES LOCATED ABROAD. The banking groups consolidating or sub-consolidating their operations in Panama and having within their structure branch or affiliated offices located abroad must make sure that those branches and offices apply measures for the prevention of money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction at least equivalent to those measures established in Panama and in the Financial Action Task Force's recommendations when the minimum requirements of the host country are less strict than those of the home supervisor's.

When the domestic regulations of the country where the companies incorporate prevent them from appropriately meeting the measures for the prevention of money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction that must be at least equivalent to those mentioned above, the banking group must inform the Superintendency.

[18] Amended by Article 16 of Rule 1-2017 dated 14 February 2017 and Article 4 of Rule 13-2018 dated 27 November 2018.

[19] Added by Article 17 of Rule 1-2017 dated 14 February 2017.

If the Superintendency of Banks considers that there is an important risk but has been unable to implement the necessary measures to remedy the situation, the Superintendency may take additional measures or impose additional controls, including ordering the closing of the operations of the (direct or indirect) branches or affiliated offices.

ARTICLE 39. PENALTY FOR NONCOMPLIANCE. Without prejudice of the penalties prescribed in Law 23 of 2015 whereby measures to prevent money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction are adopted, failure to comply with the provisions herein will be punishable by the Superintendent with a penalty of from five thousand balboas (B/.5,000.00) to one million balboas (B/.1,000,000.00), according to the seriousness or recidivism of the fault.

ARTICLE 40. ENACTMENT. This Rule shall become effective as of its promulgation.

ARTICLE 41. REPEAL. This Rule supersedes in their entirety Rule 12-2005 dated 14 December 2005, Rule 8-2006 dated 8 November 2006, Board of Directors' General Resolution SBP-GJD-0004-2014 and Board of Directors' Resolution JD-0032-2005 dated 21 December 2005.

Given in the city of Panama on the twenty-seventh (27th) day of July, two thousand and fifteen (2015).