Republic of Panama
Superintendency of Banks

RULE No. 10-2015
(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;

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. MANUAL TO PREVENT 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.

ARTICLE 4. CONFORMATION OF THE PREVENTION OF MONEY LAUNDERING COMMITTEE. 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.

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.

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. 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.

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 must maintain their database up to date and at the disposal of the Superintendency of Banks' supervisors.

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

1. To prepare a customer profile.

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

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

4. To review, at least every six (6) months, their customers' operations, both habitual and in cash of amounts 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.

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

Banks that are members of a banking group may consolidate their processes of due diligence within the compliance structure of the banking group.

ARTICLE 11. 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 the customers' risk classification and categories.

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

5. Design and description of risk matrixes.

The methodology for customer risk classification and its updates must be approved by the Prevention of Money Laundering Committee and annually submitted to the Superintendency of Banks to be verified.

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 bank is serving. In those cases 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. 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, civil 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 said document is under process, will be used in the case of a Panamanian citizen. The passport will also be acceptable for those Panamanian citizens living abroad.

   The suitable personal identification document will be the passport for foreigners. To meet this 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 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 valid 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.

2. **Customer recommendations or references:** This requisite can be met by one (1) customer and/or final beneficiary banking reference, as well as one reference for each accountholder and authorized signer for opening any bank account. This banking reference must be physically submitted or the bank must certify in the file that it has verified the banking reference provided by the customer on the relevant form.

   If the customer is referred by an entity member of the same banking group where the customer wants to conduct the operation, this one reference will suffice.

   In those exceptional cases where the customer does not have a banking reference, this requirement can be met by submitting one (1) personal or business reference provided by companies, suppliers or information agencies, e.g. the report issued by the Panama Credit Association (APC, for its acronym in Spanish) or its counterpart from other countries.

In the case of refugees, the requisite of submitting recommendations or references can be met by obtaining a letter or resolution issued by the Ministry of Government's National Office for Refugees, where the background of the person is kept.

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

4. **Customer financial profile:** 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, pay stub or any other legal or contractual documentation proving the customer's income.

   Furthermore, all reasonable measures for supporting the origin of 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 habitual behavior the customer will maintain with the regulated entity.

5. **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.

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

   1. 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 of that final beneficiary.

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

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

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

   5. 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 it represents based on the international parameters and standards and internal policies and control procedures established by the entity.

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

ARTICLE 15. 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.

   In case of trust companies, these must fully know and understand the information on the purpose of the trust fund.

2. **Customer recommendations or references:** This requisite can be met by one (1) customer and/or final beneficiary banking reference. If the customer cannot furnish a banking reference, this requirement can be met by submitting one (1) personal or business reference provided by companies, suppliers or information agencies, e.g. the report issued by the Panama Credit Association (APC, for its acronym in Spanish).

If the customer is referred by an entity member of the same banking group where the customer wants to conduct the transaction, this one reference will suffice.

3. **Certifications proving the incorporation and existence of the legal entity:** The requisite to obtain certifications proving 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 proving 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 proving the incorporation and existence of the foreign legal entity.

4. **Identification of dignitaries, directors, proxies 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 to the chairman and/or legal representative, as the case may be, secretary, people appointed as signatories and agents of the legal entity. In the case of trust companies, they must identify the protector, advisor or people making decisions on the trust fund equity and its distribution, whichever is the case.

5. **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, regulated entities must make the relevant efforts to identify shareholders holding a percentage equal or greater than ten percent (10%) of the issued shares of the relevant corporation. Listed companies, public companies and banks are exempt from identifying their final beneficiary with the exception of those incorporated countries classified as non-cooperative by the Financial Action Task Force (FATF).

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

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

6. **Source and origin of resources or equity:** It is understood that the source and origin of resources refers to the written justification on the origin of funds used to conduct any transaction.

7. **Customer financial profile:** 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: financial statements or tax return or any other legal or contractual documentation proving the customer's income.

   Furthermore, all reasonable measures for supporting the origin of 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 habitual behavior the customer will maintain with the regulated 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.

ARTICLE 16. 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 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 nominative shareholders.
    c. Copy of the share registry.

2. For corporations issuing bearer share certificates after the enactment of Law 47 of 2013, whereby a custody regime applicable to bearer shares is adopted, banks must require the customer to maintain this type of shares as follows:

    a. Copy of the minutes of the board of directors or shareholders meeting registered in the Public Registry, whereby the corporation accepts the custody regime created by Law 47 of 2013.
    b. Certification of authorized custodian proving who owns the bearer shares issued by the corporation, 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.

ARTICLE 17. SIMPLIFIED DUE DILIGENCE. Once the bank identifies the customer profile, the bank or trust company may conduct a simplified due diligence for customers identified as low risk, making sure they have gathered the following information:

1. **Customer identification and verification:** Full name, age, gender, employment or employment status, civil status, profession or occupation, citizenship, residency and a suitable personal identification document. The bank must verify the name and identification card number with the information held by the Civil Registry, as well as other data furnished by the customer.
2. Any other document that, according to the customer's type and activity, the bank deems necessary to document.

Pursuant to the parameters set forth in Rule 1-2013, simplified bank accounts are included in this risk category because they are low transaction accounts with an established quantitative threshold.

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.

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. 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. Said assessment process 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 known by the board of directors. The management must define corrective action plans to remedy proven weaknesses, stating the actions, responsible persons and terms 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. MONITORING TOOL FOR BANKS. Banks must have transactional follow up and monitoring systems that must automatically generate timely warnings on transactions different from the customer's expected behavior, 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 institution.

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

5. Warning signs generated.

The Bank must review all warning signs to identify unusual operations to which follow up must be given.

To dismiss warning signs of unusual transactions, there must be written evidence supporting the rejection of the support documentation and identifying the person responsible.

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. DUE DILIGENCE FOR HIGH-RISK CUSTOMERS. Regulated entities must adopt enhanced or reinforced due diligence measures to the customer and/or final beneficiary when classified as high-risk customers and 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 characteristics:

1. 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.

2. To conduct intensified continuous follow up on the operations throughout the contractual relation.

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

1. Politically exposed persons (PEP).

2. Customers using high 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 bank 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. KNOW YOUR EMPLOYEE POLICY. Banks and trust companies must appropriately choose 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.

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.
    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. SUSPICIOUS OPERATIONS. Banks and trust companies must directly inform the Financial Analysis Unit of any suspected event, transaction or operation that may be related or involved with money laundering crimes, regardless of the amount and whether it can be confirmed, as well as any control failure.

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 regulated entities are aware, during the course of their activities, that there were operations classified as suspicious operations that cannot be confirmed, they must comply with the following actions:

1. To create a log containing operational information. The information will contain the data of 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. To notify the Compliance officer of the suspicious operation. He will order a review of the operation to verify its "suspicious" condition and will succinctly include the relevant remarks.

3. To 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 Compliance officer within fifteen (15) calendar days following the detection of the suspicious event, transaction or operation. Nevertheless, regulated entities can request the Financial Analysis Unit (UAF) grant an extension of fifteen (15) calendar days to submit supporting documentation in cases where there is any complication in gathering the information.

4. To 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. To update the relevant file in the case of suspicious operations.

6. If necessary, to 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. INTERNAL AUDITING. The Bank's internal auditing unit is responsible for continuously assessing and following up on the internal control system and compliance of Money Laundering risk management policies.

ARTICLE 38. BANKING GROUPS. The shareholder of banking groups to which the Superintendency of Banks is the home supervisor must make sure to comprehensively manage group-level money laundering risk, as well as assessing the potential risks associated with the activities notified 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 make sure that he banking group applies rules and procedures equivalent to those adopted by the bank, especially with regard to customer due diligence measures.

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 fifteen (2015).

FOR COMMUNICATION, PUBLICATION AND ENFORCEMENT.

THE CHAIRMAN, **THE SECRETARY,**

Luis Alberto La Rocca L. J. Montague Belanger