**Republic of Panama**
**Superintendency of Banks**

# OTHER REPORTING ENTITIES AML RULE N°. 5-2018
**(dated 11 December 2018)**

**"Whereby the guidelines for preventing the misuse of services provided by exchange bureaus are established"**

**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 re-edited Decree Law 9 dated 26 February 1998 and all its amendments as a consolidated text, and this text was approved by means of Executive Decree 52 dated 30 April 2008, hereinafter referred to as the Banking Law;

Pursuant to the provisions of paragraph 1 of Article 5 of the Banking Law safeguarding the soundness and efficiency of the banking system is one of the objectives of the Superintendency of Banks;

Pursuant to the provisions of 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 one of the objectives of the Superintendency of Banks;

Article 112 of the Banking Law establishes that banks and other entities supervised by the Superintendency are required to establish policies and procedures and the internal control structures to prevent their services being misused 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 provides 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 required to submit this information to the Superintendency whenever it may so require;

According to the provisions of 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 relevant standards in accordance with policies and regulations in force in the country;

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

Article 19 of Law 23 dated 27 April 2015 establishes the Superintendency of Banks as a supervisory body;

Paragraph 7 of Article 20 of Law 23 of 2015 provides that issuing guidance and feedback standards to the financial reporting entities, the nonfinancial reporting entities and activities performed by professionals subject to supervision for its enforcement, as well as the procedures for the identification of the final beneficiaries, legal entities and other legal structures, is among the duties of the supervisory bodies;

According to the provisions of Law 23 of 2015 on the prevention of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction, the Superintendency of Banks will be responsible for supervising and regulating other reporting entities on the prevention of money laundering, in addition to the banks and trust companies already under its supervision;

Article 22 of Law 23 of 2015 establishes the financial entities to be supervised by the Superintendency of Banks for the prevention of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction;

By means of Article 123 of Law 21 dated 10 May 2017, Article 22 of Law 23 of 2015 was amended, adding the money service businesses as new reporting entities that the Superintendency of Banks will be responsible for regulating and supervising for the prevention of money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction;

By means of Rule 8-2017 dated 19 September 2017, by means of which Article 1 of Rule 5-2015 dated 26 May 2015 for the prevention of the misuse of services provided by other reporting entities was amended, exchange bureaus are included as new reporting entities that the Superintendency of Banks will be responsible for regulating and supervising under the provisions of Rule 5-2015;

During the Board of Directors' working sessions it was determined that it was necessary and advisable to have a specific rule establishing the guidelines for preventing the misuse of services provided by exchange bureaus and fitting the special nature of this type of business. This requires special regulations recognizing the vulnerabilities and risks of money laundering inherent in the activity establishing measures for prevention and mitigation based on the risk-based approach to that type of activity.

**RESOLVES:**

**ARTICLE 1. SCOPE.** According to the provisions of Article 22 of Law 23 of 2015 whereby the measures to prevent money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction, the provisions herein will be applied to exchange bureaus of any type, whether operating by physical delivery or purchase of future contracts and whether or not it is their main activity.

**ARTICLE 2. DEFINITION.** For the purposes of the provisions of this Rule and without prejudice to the definitions established in other legal provisions, the following terms will be understood as:

1. **Exchange bureaus:** Any individual or legal entity providing services for purchasing and selling currency, paper money or other monetary instruments within or outside the country, in any form, whether or not it is their main activity;

2. **Concentration account:** A bank or deposit account that an exchange bureau opens in any bank to receive money from its customers;

3. **Monetary instrument:** Paper money or coins of legal tender in Panama or any other country, traveler's checks, precious metals, domestic and foreign checks, and any other type of resources, rights, property or goods.

**ARTICLE 3. PREVENTION OF MONEY LAUNDERING, THE FINANCING OF TERRORISM AND THE FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION BY EXCHANGE BUREAUS.** The exchange bureaus must take the necessary measures, pursuant to the risk-based approach, to prevent their operations and/or transactions being conducted with funds or on funds coming from activities associated with the crimes of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction. Therefore, they are required to meet the terms established in the legal provisions and those herein related to that matter.

In connection with the above, the exchange bureaus must prepare a manual for the prevention of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction that must contain the policies, mechanisms, procedures, controls and measures that will be adopted for preventing their services being used with funds coming from these activities.

As a result, the exchange bureaus must draft a document containing the policies, criteria, measures and internal procedures establishing a methodology designed and implemented to conduct an assessment of the risk to which they are exposed as a consequence of the services they render, the jurisdictions where they have operations, the customers with which they conduct transactions, the amounts of the transactions and the distribution channels with which they

maintain operations. This risk-based approach methodology must establish the processes for the identification, measurement and mitigation of identified risks.

The document containing these policies must be approved by the signature of the top management or legal representative and must be made available to the Superintendency for supervision purposes. The person in charge of policy implementation must be the Compliance Officer.

The manual must be disseminated to all members of the exchange bureau staff.

**ARTICLE 4. "CUSTOMER" CONCEPT.** For the purposes of this Rule, the customer will be understood as any individual that establishes, maintains or has maintained a formal or casual contractual or business relationship with an exchange bureau.

**ARTICLE 5. CUSTOMER DUE DILIGENCE.** The exchange bureaus will identify and verify, through reliable documents, the identity of the individuals intending to conduct transactions within the exchange bureau. For these purposes, the exchange bureaus will request the following information and documentation from all of its customers before commencing a business relationship: full name, date of birth, profession or occupation, address, telephone number, e-mail, and suitable personal identification document. For the purposes of the suitable identification document, the personal identification card will suffice for a Panamanian citizen. For a foreigner, the personal identification document will be the passport with a photograph of the holder.

If the customer conducts a single transaction or various remittance and reception transactions totaling an amount equal to or greater than one thousand balboas (B/.1,000.00) in a calendar week, the exchange bureau must prepare a form designed by the entity containing information in writing or electronically, as well as [retaining] the documents verifying the information:

1. **Source of resources or assets:** Refers to the written evidence on the origin of funds used to conduct a transaction, information that can be documented with an affidavit from the customer.

2. **Origin and destination of resources or assets:** Refers to the origin and destination of money, the jurisdiction from where it is received or to where it is sent. In the case of the destination, it will always mean the geographical location and the treatment that should be given within the risk matrix and the customer risk classification, taking into consideration the geographic criteria along with the nationality, country of birth and other elements that are deemed relevant.

**ARTICLE 6. ADDITIONAL DUE DILIGENCE MEASURES.** In all cases, exchange bureaus must take into consideration the following aspects when conducting customer due diligence:

1. The exchange bureaus must establish controls or reasonable measures to prevent conducting operations on behalf of third parties or beneficiaries other than the owner of the operation;

2. The exchange bureaus must only provide their products and services to individuals;

3. The exchange bureaus must have documented evidence in the relevant file of all actions taken to appropriately identify the customer;

4. The exchange bureaus must prepare a customer risk matrix pursuant to international standards and domestic regulations;

5. If the customer cannot or refrains from providing the requested documentation, the reporting entity must not conduct the operation, registering it as "not executed," along with any data it was able to obtain;

6. All customer due diligence information must be consolidated in a single physical or digital file by customer.

The reporting entities must identify and verify the customer by requesting and consulting documents, data, or reliable information from independent sources, such as software or tools consolidating domestic and international information related to the prevention of money laundering (e.g. OFAC list, UN list, among others).

**ARTICLE 7. METHODOLOGY FOR CUSTOMER RISK CLASSIFICATION.** Each exchange bureau must design and adopt a methodology for customer risk classification that must contain the following elements, as a minimum:

1. General concept;

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

3. Description of the customer risk classification and categories;

4. Description of the models for establishing the customer risk profile;

5. Design and description of the risk matrixes;

6. Definition of the procedure for updating the customer risk classification, which must contain the authorization to make changes to the customer risk classification. In the event the customer risk classification is determined by an automated monitoring tool, the entity must ensure that the system keeps the evidence of each change made in the customer risk profile, which must be captured in the established procedure.

The customer risk classification methodology and its updates must be approved at least once a year and submitted on an annual basis to the Superintendency of Banks by the Chief Executive Officer with the ratification of the Board of Directors or the legal representative of the organization holding the registration with the Superintendency.

Since it is understood that the application of the customer assessment risk matrix must be effective and demonstrate a statistical correlation between the variables of the transacted amount by the customer and the risk level assigned (except for regulatory criteria such as the requirements for PEPs), the reporting entity must demonstrate in each case that the monitoring tool, the customer identification information, the transactions conducted in the calendar week and the level of risk assigned are congruent.

The Superintendency of Banks will make the necessary efforts to verify that the customer risk classification method is reasonable according to the volume and nature of the transactions the reporting entity conducts, as well as the risk profile of the customer served.

In cases where it is determined that the classification methodology is insufficient or inappropriate, the Superintendency can require the reporting entity take the relevant corrective or clarification measures within a period the Superintendency may establish.

The exchange bureaus must clearly establish the methodology they use for monitoring and assigning the risk level; in all cases, the operations to be considered are those produced locally and abroad. Only the transactions going through the entity registered with the Superintendency may be considered within the referred statistical validation, regardless of the operations that its parent company may conduct globally.

**ARTICLE 8. MINIMUM CRITERIA OR VARIABLES TO ANALYZE AND DESCRIBE THE CUSTOMER RISK PROFILE.** To analyze and describe the customer risk profile, the exchange bureaus must apply the following criteria, as a minimum:

1. Nationality;

2. Country of birth;

3. Country of domicile;

4. Geographic zone of the customer’s business activities;

5. Customer economic and financial activity;

6. Type, amount and frequency of transactions;

7. Whether it is a politically exposed person (PEP);

8. Products, services and channels the customer uses;

9. Type of monetary instrument.

The criteria or variables used for the analysis and description of the customer risk profile must be described in the methodology for customer risk classification that the exchange bureau uses and demonstrate statistically that it meets the requirement to separate customers by their risk level in a way that is reasonable and suitable to the operations profile of the exchange bureau.

**ARTICLE 9. EXCHANGE BUREAU RISK ASSESSMENT.** The money laundering risk assessment is an integral part of the methodology for the exchange bureau risk assessment. The assessment methodology must be conducted by the area appointed by the Board of Directors or the legal representative of the organization holding the registration with the Superintendency, with the participation of the area [responsible] for the prevention of money laundering, and must be approved by the board of directors or the legal representative of the entity.

The result of the application of the risk assessment methodology must be reviewed at least once every twelve (12) months and the results obtained must be presented to the board of directors and/or the legal representative. The management must define corrective action plans to remedy any identified weaknesses, indicating the actions, the persons responsible and the timeline for the corrective action. The mechanisms approved for compliance verification must be recorded in the board of directors meeting minutes and/or agreement meeting minutes attended by the legal representative. This methodology and the result of the risk assessment must be submitted on an annual basis to the Superintendency of Banks.

**ARTICLE 10. DOCUMENTATION AND FOLLOW-UP.** The exchange bureaus must keep all customer information and follow up on the transactions conducted by the customer during the course of the business relationship in order to identify unusual operations. The reporting entities must have tools to detect abnormal or suspicious activity patterns in all relations maintained with the customers.

**ARTICLE 11. PREVENTIVE FREEZING.** For the purpose of the provisions of Article 49 of Law 23 of 2015, the exchange bureaus must develop policies and procedures for managing the preventive freezing of resources or assets held by them and belonging to persons included in the relevant lists issued by the United Nations Security Council.

In addition, the exchange bureaus must develop policies and procedures for prohibiting operations being conducted with resources or assets belonging to persons included in the lists issued by the United Nations Security Council.

**ARTICLE 12. POLITICALLY EXPOSED PERSONS (PEPs).** The exchange bureaus must adopt an enhanced or reinforced customer due diligence measure for individuals classified as politically exposed persons, whether national or international, pursuant to the provisions of paragraph 18 of Article 4 of Law 23 of 2015.

A person will be considered a PEP from the moment he/she is appointed until he/she steps down from the position and for a period of two (2) years from the moment he/she ceases to discharge the duties and obligations for which that person was initially classified as a PEP.

The exchange bureaus must establish appropriate systems for risk management and conduct deeper due diligence, pursuant to the provisions of Article 34 of Law 23 of 2015.

**ARTICLE 13. DUE DILIGENCE FOR HIGH-RISK CUSTOMERS.** The exchange bureaus must adopt an enhanced or reinforced customer due diligence measure for customers classified as high-risk, as well as to take pertinent measures for these customers.

For people classified as high-risk, the reporting entities must establish appropriate systems for risk management and conduct an enhanced or reinforced due diligence including the following facets:

1. Obtain top management’s approval to establish (or update the profile in case of existing customers) business relationships with these customers, when applicable;

2. Conduct intensified, ongoing monitoring of the operations.

Without prejudice to the customers that, according to the exchange bureau risk assessment, are considered high-risk customers, [the following persons] will be considered to be in this category:

1. Politically exposed persons (PEPs);

2. Customers conducting individual or cumulative operations in a calendar week equal to or greater than one thousand balboas (B/.1,000.00);

3. Customers with capital or business associates coming from territories or countries considered non-cooperative jurisdictions by the Financial Action Task Force (FATF);

4. Any other customer classified as high-risk by the reporting entity.

**ARTICLE 14. STATEMENT OF CASH OR QUASI-CASH TRANSACTIONS.** The exchange bureaus must declare the following transactions or operations, as well as any other additional information related to these, on the forms provided by the Financial Analysis Unit, whether or not conducted in or from the Republic of Panama:

1. Single operations conducted by individuals for the amount of ten thousand balboas (B/.10,000.00) or more. Operations in foreign currency must be reported in the dollar/balboa equivalent;

2. Multiple monetary operations which, although individually below ten thousand balboas (B/.10,000.00), total ten thousand balboas (B/.10,000.00) or more at the end of the day or the week. If this is the case, the exchange bureau will report the operation for its cumulative value at the end of the business week, through the means provided by the Superintendency of Banks for that purpose. The reporting entity must maintain in its records and available to the Superintendency of Banks, the documentation proving the timely and accurate submittal of the data contained in the statements referred to in this subparagraph;

3. The exchange of cash in low denominations for others in high denominations or vice-versa for the amount of ten thousand balboas (B/.10,000.00) or more, or through multiple transactions that, although individually are for amounts below ten thousand balboas (B/10,000.00), at the end of the day or week total ten thousand balboas (B/.10,000.00) or more;

4. The exchange of cashier's or traveler's checks, money orders, bearer checks, checks with blank endorsements or issued on the same date or close dates by the same drawee or drawees of the same market;

5. The purchase or sale of currency other than the legal tender in the Republic of Panama equivalent to then thousand balboas (B/.10,000.00) or more or the sum of this amount in a week, or through successive transactions that, although individually are for amounts below then thousand balboas (B/.10,000.00), at the end of the day or week total ten thousand balboas (B/.10,000.00) or more, must be reported in the dollar/balboa equivalent.

**ARTICLE 15. REVIEW, UPDATE AND RECORDKEEPING.** The exchange bureaus must maintain all information records and documentation obtained during the due diligence process up to date. They will also keep a signed set of the due diligence forms or the electronic archive of the data that were obtained from the individual, a hard or scanned copy of documents obtained through the due diligence process, the documents verifying the operation or transaction and any other document that permits reconstructing every customer operation or transaction, when appropriate, for a five-year period from the date the contractual relation with the customer was terminated, through any means authorized by Law.

The documents and data on the customers must be updated pursuant to the policy each reporting entity adopts for the customers that do not have any variation in their risk profiles.

**ARTICLE 16. KNOW YOUR EMPLOYEE POLICY.** The exchange bureaus must appropriately choose [their employees] and supervise their behavior, especially of those holding positions related to customer service, receipt of money and control of information. In addition, the exchange bureaus must maintain an employee profile that must be updated on an annual basis while the work relationship lasts.

The employees must be trained to understand the risks to which they are exposed, the controls mitigating these risks and the personal and organizational impact of their actions.

Additionally, the employees, managers and directors of the exchange bureaus must have available a code of conduct that provides a benchmark for their behavior 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 exchange bureaus must] establish measures to ensure the duty to maintain confidential the information related to the system for the prevention of money laundering.

The code of conduct or document establishing the work relationship must contain, as a minimum, the guiding principles, values and policies aimed at highlighting the compulsory character of the procedures making up the AML/CFT/PWMD system and its appropriate development, according to the existing regulations on that matter. Additionally, they must establish that any breach to the AML system will be considered an infraction that will be punished according to the severity of the non-compliance.

**ARTICLE 17. REQUIREMENT TO TRAIN EMPLOYEES.** The exchange bureaus must provide ongoing and specific training to the employees of the business and operating areas in positions related to treating, communicating and dealing with customers, suppliers, receipt of money, processing transactions and designing products and services, as well as the staff working in sensitive areas such as compliance, risk, human resources, technology and internal auditing (if applicable). This training will be aimed at maintaining [personnel] current on the different crimes, cases and regulations on money laundering, which must be conducted for:

1. **Orientation for new employees:** The reporting entities must develop and implement orientation training on the prevention of money laundering for new employees that must be developed before or simultaneously with the commencement of work at the reporting entity. This training must include, as a minimum, the following topics:

    **a.** Fundamentals of the prevention of money laundering;

    **b.** Current regulations on the prevention of money laundering;

    **c.** Contents of the Compliance Manual;

    **d.** Customer due diligence and know your customer procedures;

    **e.** Red flags and crimes applicable to the sector in which they operate;

    **f.** Criminal, administrative and internal responsibilities and penalties.

2. **Annual training for the entity's staff as provided for in this Article:** The exchange bureaus must develop and implement an annual training program in order to keep the existing staff updated on the policies, procedures and internal controls to prevent the misuse of the services they render, as well as the methods criminals use for money laundering. This training must also include the following:

    **a.** Procedures adopted by the entities to comply with the provisions contained in this Rule;

    **b.** Analysis of the existing regulation, including the implications for the reporting entity and its employees;

    **c.** Responsibilities of the Auditing and Compliance Departments and the Business areas;

    **d.** Recommendations from international organizations;

    **e.** Analysis and development of current cases related to money laundering crimes;

    **f.** The importance of maintaining communication with the Compliance Officer; channels and type of information that must be provided in investigations that need to be conducted.

The training programs conducted by exchange bureaus must include mechanisms for evaluating the results obtained, in order to determine the efficiency of these programs and the scope of the proposed objectives. There must be a record of the training provided to the employees, as well as the date, time, place and duration of the activity, the names of the attendees, the positions they hold and the contents of the training.

The statistics on the evaluation of this training must be reported to the Chief Executive Officer in order to guarantee the relevant corrective actions. There should be defined criteria establishing the action to be taken for the employees that do not successfully complete the evaluation of knowledge.

**ARTICLE 18. INFORMATION TECHNOLOGY SYSTEM.** The exchange bureaus must have in place an information technology system with an option that will permit the Superintendency to validate compliance with the provisions established in this Rule and those provided on the prevention of money laundering through integral and destructive tests. This option must consist on an exact replica of the operating system with mirrored data.

**ARTICLE 19. MONITORING TOOL.** The exchange bureaus must have effective transactional follow-up and monitoring systems consistent with their products, geography, customers and channels, which must produce red flags automatically and in a timely manner on transactions deviating from the expected customer behavior, and others that permit the identification of various crimes, as well as reports including, as a minimum, but not limited to, the following:

1. Customer data;
2. Transaction records;
3. Types of transactions;
4. Existing correlation with other products and services within the exchange bureau;
5. A record of the risk classification assigned to each customer;
6. Red flags generated;
7. Statistics on the red flags generated, processed, under process, and pending to be processed, with the relevant supporting documentation.

The reporting entity must appoint a suitable and responsible person as monitoring tool administrator.

The exchange bureaus must review all red flags in order to identify unusual transactions for follow-up.

For unusual transactions that are ruled out, there must be evidence of the reasons for ruling them out and the supporting documentation must be kept in either hardcopy or digital form.

**ARTICLE 20. UNUSUAL TRANSACTIONS.** The exchange bureaus must do an in-depth analysis of unusual operations to obtain additional information that permits them to corroborate or rule out the unusual [nature of the transaction], leaving a written record of the conclusions and the verified supporting documentation.

When the reporting entity identifies an unusual transaction, it must start an investigation on the described event containing the following data:

1. Customer identification;
2. Economic activity;
3. Background of the operation, e.g. record of the transactions, locations, among others;
4. Detailed description of the surveyed or analyzed movements or transactions;
5. Conclusions and recommendations on the analyzed case.

The exchange bureaus must create a registry of unusual operations it investigates, to include those that they determine are not reportable as suspicious operations.

**ARTICLE 21. SUSPICIOUS TRANSACTIONS.** The exchange bureaus must directly inform the Financial Analysis Unit of any event, transaction or operation that the former suspects may be related or linked to money laundering crimes, regardless of the amount, and that could not be justified and supported, as well as any failures in controls.

The Compliance Officer must conduct an internal analysis of the unusual and/or suspicious transactions resulting from comparing the customer profile and/or its monitoring systems.

During the course of their activities, when the exchange bureaus become aware of transactions that qualify as suspicious and that cannot be justified or supported, they must take the following actions:

1. Create a record of the information on the transaction. The information will contain the data of the commercial relationship and the information originating the transaction, the date(s), the amount(s), and the type(s) of transaction. This record must include succinctly the remarks made by the employee detecting the operation;

2. Report the suspicious transaction to the Compliance Officer, who will order a review of the transaction to verify that it is suspicious and will succinctly include the relevant remarks;

3. Report the suspicious transaction to the Financial Analysis Unit for the Prevention of Money laundering and the Financing of terrorism (UAF, for its acronym in Spanish) in the forms established for that purpose. The notification will be conducted through the Compliance Officer within fifteen (15) calendar days following the detection of the suspicious event, transaction or operation. However, reporting entities can request a fifteen (15) calendar day extension from the Financial Analysis Unit (UAF) for the submittal of the supporting documentation when gathering the information is difficult;

4. Register in the logbook the date and reporting format of the report sent to the Financial Analysis Unit for the Prevention of Money Laundering and the Financing of Terrorism (UAF), as well as the date and reference number of the Unit’s response;

5. In the event of suspicious transactions, update the relevant file;

6. If applicable, charts, tables, news and other information that permit the visualization of the suspicious transactions being reported should be attached.

**ARTICLE 22. REPORTING TO THE FINANCIAL ANALYSIS UNIT (UAF).** The Superintendency of Banks will inform the Financial Analysis Unit (UAF) of any suspicious transactions it notices during the examinations of exchange bureaus, without exempting the entity from the obligation of doing so.

**ARTICLE 23. PROTECTION OF EMPLOYEES AND DIRECTORS.** The exchange bureaus will adopt appropriate measures to maintain confidentiality on the identity of employees or directors that have communicated or reported information to the internal prevention bodies of the reporting entity.

**ARTICLE 24. CORPORATE LIABILITY.** For the sole purpose of sanctions, the actions and conduct of the directors, dignitaries and executive, administrative or operations personnel of the exchange bureau shall be attributable to these entities and to the individuals on whose behalf they are acting.

The individuals who commit such acts and conduct are subject to the relevant civil and criminal liabilities.

**ARTICLE 25. INDEPENDENT AUDIT.** The independent audit for this type of reporting entity will be conducted by an internal or external agent and will be responsible for the ongoing assessment and follow-up on the internal control system and compliance with the money laundering risk management policies.

The management of auditing duties must be independent and the external auditor or staff must be suitable and well-trained in matters of the prevention of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction. The exchange bureaus must ensure that the external auditor or staff has the experience in risk-based approach auditing.

**PROVISO:** For the purposes of the provisions of Law 23 of 2015, the exchange bureaus must have a written opinion on the assessment and continuous monitoring of the internal control systems for the prevention of the crimes of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction. The independent audit opinion must comply with the provisions established in this Article. The independent audit or evaluation on the efficiency of controls established in that matter must be made annually and the results will be an integral part of the reports that reporting entities must maintain and submit upon the Superintendency's request.

**ARTICLE 26. BRANCH OFFICES ABROAD.** The exchange bureaus consolidating or sub-consolidating their operations in Panama and with branch offices abroad within its structure must make sure that these branch offices apply measures for the prevention of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction at least equivalent to those established in Panama and by the Financial Action Task Force recommendations when the minimum requirements of the host country are less stringent than that of the home supervisor.

When the domestic legislation of the country where the branch offices are incorporated prevent due compliance with the measures for the prevention of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction that must be at least equivalent to those indicated in the above paragraph, the exchange bureau must inform the Superintendency of this situation.

If the Superintendency of Banks deems there is significant risk and it is not possible to adopt measures to remedy the situation, the Superintendency may require additional measures or controls, including ordering the closure of operations of that branch office.

**ARTICLE 27. FINES FOR NONCOMPLIANCE.** Without prejudice to the fines prescribed in Law 23 of 2015 adopting measures for the prevention of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction, failing to comply with the provisions of this Rule will be penalized by the Superintendent with fines from five thousand balboas (B/.5,000.00) up to one million balboas (B/.1,000,000.00), according to the severity of the offense or the degree of recidivism.

**ARTICLE 28. ENACTMENT.** This Rule will become effective on 1 July two thousand nineteen (2019).

Given in the city of Panama on the eleventh (11th) day of December, two thousand eighteen (2018).

**FOR COMMUNICATION PUBLICATION AND ENFORCEMENT.**

**THE CHAIRMAN,** **THE SECRETARY,**

Luis Alberto La Rocca Joseph Fidanque III